Naval Education and Training Command

NAVEDTRA 12845
April 1997
0502-LP-003-5230

Training Manual (TRAMAN) and Nonresident Training Course (NRTC)

Radioman Training Series

Module 1—Administration and Security

Only one answer sheet is included in the NRTC. Reproduce the required number of sheets you need or get answer sheets from your ESO or designated officer.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

The public may request copies of this document by following the purchasing instruction on the inside cover.

0502LP0035230

Although the words “he,” “him,” and “his” are used sparingly in this manual to enhance communication, they are not intended to be gender driven nor to affront or discriminate against anyone reading this text.

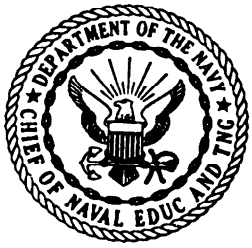
DISTRIBUTION STATEMENT A Approved for public release; distribution is unlimited.

The public may request copies of this document by writing to Superintendent of Documents, Government Printing Office, Washington, DC 20402-0001 or to the Naval Inventory Control Point (NAVICP) - Cog “I” Material, Attention Cash Sales, 700 Robbins Avenue, Philadelphia, PA 19111-5098.

RADIOMAN TRAINING SERIES

MODULE 1—ADMINISTRATION AND SECURITY

NAVEDTRA 12845



1997 Edition Prepared by
RMCS(SW/AW) Deborah Hearn and
DPC(SW) Walter Shugar, Jr.

PREFACE

This training manual (TRAMAN), together with its nonresident training course (NRTC), NAVEDTRA 12845, form a self-study training package for personnel fulfilling the requirements of the Radioman rating. The TRAMAN provides subject matter that relates to the occupational standards for the RM rating. The NRTC consists of several assignments to help the student complete the TRAMAN.

This edition includes information on AIS administration, communications administration, communications security, AIS security, and general security.

This training manual was prepared by the Naval Education and Training Professional Development and Technology Center, Pensacola, Florida, for the Chief of Naval Education and Training.

1997 Edition

Stock Ordering No.
0502-LP-003-5230

Published by
NAVAL EDUCATION AND TRAINING PROFESSIONAL
DEVELOPMENT AND TECHNOLOGY CENTER

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON, D.C.: 1997

THE UNITED STATES NAVY

GUARDIAN OF OUR COUNTRY

The United States Navy is responsible for maintaining control of the sea and is a ready force on watch at home and overseas, capable of strong action to preserve the peace or of instant offensive action to win in war.

It is upon the maintenance of this control that our country's glorious future depends; the United States Navy exists to make it so.

WE SERVE WITH HONOR

Tradition, valor, and victory are the Navy's heritage from the past. To these may be added dedication, discipline, and vigilance as the watchwords of the present and the future.

At home or on distant stations we serve with pride, confident in the respect of our country, our shipmates, and our families.

Our responsibilities sober us; our adversities strengthen us.

Service to God and Country is our special privilege. We serve with honor.

THE FUTURE OF THE NAVY

The Navy will always employ new weapons, new techniques, and greater power to protect and defend the United States on the sea, under the sea, and in the air.

Now and in the future, control of the sea gives the United States her greatest advantage for the maintenance of peace and for victory in war.

Mobility, surprise, dispersal, and offensive power are the keynotes of the new Navy. The roots of the Navy lie in a strong belief in the future, in continued dedication to our tasks, and in reflection on our heritage from the past.

Never have our opportunities and our responsibilities been greater.

CONTENTS

CHAPTER

1. AIS Administration 1-1

2. Communications Administration 2-1

3. Communications Security 3-1

4. AIS Security 4-1

5. General Security 5-1

APPENDIX

I. Glossary . . . . . .AI-l

II. Glossary of Acronyms and Abbreviations AII-1

III. References Used to Develop the TRAMAN AIII-1

I N D E X INDEX-1

SUMMARY OF THE RADIOMAN TRAINING SERIES

MODULE 1

Administration and Security—This module covers Radioman duties relating to administering AIS and communication systems. Procedures and guidance for handling of classified information, messages, COMSEC material and equipment, and AIS requirements are discussed.

MODULE 2

Computer Systems—This module covers computer hardware startup, including peripheral operations and system modification. Other topics discussed include computer center operations, media library functions, system operations, and troubleshooting techniques. Data file processes, memory requirements, and database management are also covered.

MODULE 3

Network Communications—This module covers network administration, LAN hardware, and network troubleshooting. Related areas discussed are network configuration and operations, components and connections, and communication lines and nodes.

MODULE 4

Communications Hardware—This module covers various types of communications equipment, including satellites and antennas. Subjects discussed include hardware setup procedures, COMSEC equipment requirements, distress communications equipment, troubleshooting equipment, satellite theory, and antenna selection and positioning.

MODULE 5

Communications Center Operations—This module covers center operations, including transmit message systems, voice communications, center administration, quality control, and circuit setup/restorations. Guidelines for setting EMCON and HERO conditions and cryptosecurity requirements are also discussed.

CHAPTER 1

AIS ADMINISTRATION

LEARNING OBJECTIVES

Upon completing this chapter, you should be able to do the following:

- *Describe the preparation and monitoring of the run schedule.*
- *Examine console printouts, logs, and describe the analysis of console printouts and logs.*
- *Schedule computer downtime with users, to include hardware maintenance and software upgrades.*
- *Prepare emergency urgent change requests, to include application and system programs.*
- *Prepare, review, and coordinate trouble reports.*
- *Describe how to conduct and update an AIS equipment inventory.*
- *Describe the preparation and analysis of system performance reports.*
- *Explain the establishment and maintenance of system resource limits.*
- *Describe how to project future application growth capabilities.*
- *Explain how to prepare guidelines for contingency/disaster recoveries, to include adequate replacement parts and backup media and current backups.*

Are scheduling systems really necessary to get the work done? No; but unless you are working at an AIS facility with unlimited resources, it would not be long before confusion and disorder set in if you did not have one. That would be followed by unhappy and dissatisfied users demanding their output products in a timely manner. Users rely on computer operations and support personnel to get their jobs done on time.

Whether your AIS facility has one or several computers, it will be your job to see that the AIS production work of your command is processed in a timely reamer. This means schedules. You will need to develop monthly production schedules in coordination with user-assigned subsystem coordinators. You will also need to develop daily workload schedules to meet user-established deadlines. If your computer system has online capabilities, you will need to be sure users have access when they need it and that the system is responsive.

Technical administration and support are important aspects of automated information system (AIS) facility management. As a technical administrator, you will be making hardware and software projection reports, software performance reports, hardware utilization reports, and trouble reports. You will be responsible for

implementing performance-tuning initiatives to improve computer system performance. You will also be expected to project future application growth capabilities. All these are technical functions needed to ensure the smooth operation of an AIS facility.

In this chapter, you will learn about the many varied tasks you may perform as an input/output control clerk and then as a scheduler, reports preparation, trouble reports, technical assists, and operational guidelines. Our objective is to give you a better understanding of the importance, scope, and responsibilities that go with processing production jobs—receiving jobs, scheduling AIS production within the AIS facility, and ensuring the accuracy and timeliness of products.

I/O CONTROL

I/O control is the interface between the user and the computer system. Figure 1-1 shows an example of the role played by I/O control in the processing of computer jobs.

I/O CONTROL PROCEDURES

I/O, as you know, stands for input/output. The people who perform I/O functions are called control clerks, I/O control clerks, job-staging clerks, distribution clerks, or computer aids. In short, these are the people who are responsible for the quality and control of data processing input and output media and products. They ensure that the data to be processed meets all the requirements as outlined in the input criteria (instructions and procedures), that all data are processed, that all processing steps are performed, that the output products are distributed to the appropriate users once they are complete.

To be an efficient and effective I/O control clerk, you should be able to work on your own with a minimum of supervision; work well with other people; display tact and diplomacy; be a good communicator; use sound judgment; be logical, methodical, and persuasive; and most of all be able to respond to users' requests. Although you may manage to stay out of the limelight in this job, you do perform an integral function in the overall ADP operation. The importance and impact you have (whether it be aboard ship or ashore) is far-reaching and invaluable. Most opinions formulated by the AIS users (customers) are based on the quality of their output products and their personal contact with you as an I/O control clerk. Your attitude toward your job and its importance is seen not only by the customer, but also by your fellow workers, supervisor, and, in some cases, management. The quality of your work will be your signature when dealing with other AIS personnel and customers.

I/O control is a process. Your job will be to follow your installation's procedures. Although the procedures may differ from one installation to another, they all require the same knowledge and skills.

As an I/O control clerk, you act as the middle person between the user (customer) and the computer. Normally, the users come to you with a transmittal or request form and sometimes with their input—source documents, magnetic tapes, diskettes, and so on. Before accepting and logging in their jobs, take a few moments to look over the transmittal form. Be sure that all the necessary entries are properly filled in, that they are readable, and that any special instructions are understandable. It is better to clear up any misunderstandings right then and there, rather than having to contact the user again later and possibly cause a delay in the job getting on the computer. Never be embarrassed to ask questions. You must remember that many of the users you come in contact with are non-ADP oriented; therefore, it is up to you to help them understand the process and its requirements.

Once you have logged the job in, you may work with data entry to prepare data or programs; then with the media library to pull the needed tapes or disks; and then with computer operations to have the job run. Once the job has been run on the computer, you may check the output products. When you are sure the outputs are OK, you distribute them according to instructions, log the job out, and file or return the job materials to the user.

Study figure 1-1 for a few moments. It will help you see how the work flows and how you, as an I/O control clerk, fit in the picture. The fictional areas are listed across the top of the figure.

As you enter the level of middle management, you will be required to take on added duties and additional responsibilities. You will be a technical administrator, and you will provide support to management. You will use your expertise to evaluate current procedures and equipment and to make recommendations for improvements to operations. This includes estimating future equipment needs.

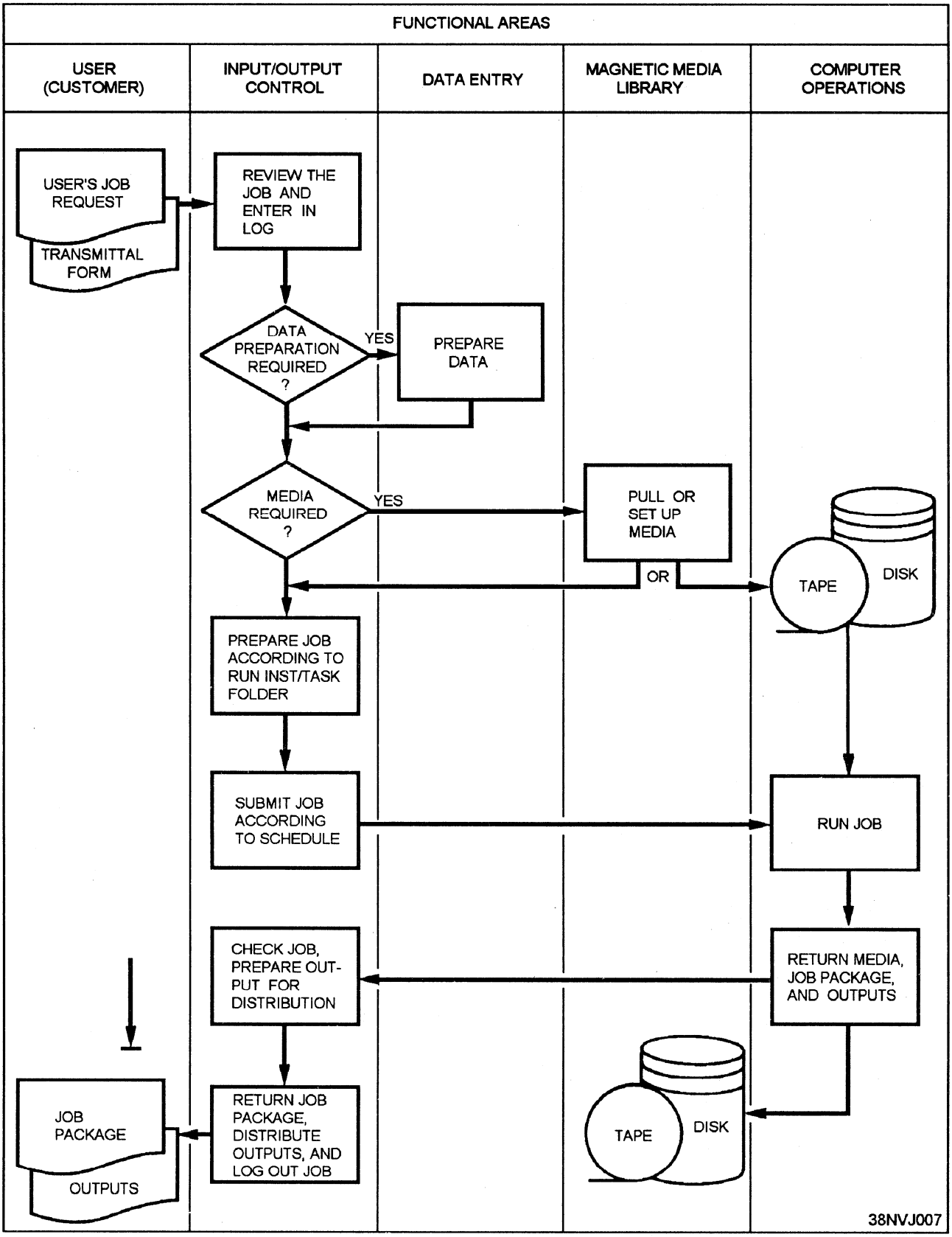


Figure 1-1.—Typical I/O control workflow.

OPERATIONAL REQUIREMENTS

Your operational requirements will include some or all of the following tasks:

- Receive user job requests.
- Maintain input and output control logs.
- Verify inputs to be processed to ensure they are correct and in accordance with the run folder or run instructions.
- Make system control language (SCL) run stream changes as required for correct data processing of the user's runs.
- Input the user's run package (jobs) to the computer operations personnel according to a schedule.
- Monitor the jobs in progress to ensure that all data are processed and that all processing steps have been properly performed.
- Balance the number of records input relative to the number output.
- Verify the format and the number of copies of each printed output in accordance with instructions in the run folder.
- Reconcile processing discrepancies and inconsistencies.
- Ensure that printed outputs are complete, properly collated, and assembled.
- Arrange for distribution of outputs to authorized users.
- Operate a variety of auxiliary equipment: copying machines, decollators, tape cleaners, CRT terminals, and so on.
- Become familiar with the basic operations of the AIS computer facility.

Now that you are familiar with the process and with operational responsibilities, let's look at the parts: transmittal forms, input control logs, job preparation, scheduling, monitoring, and output products.

Processing AIS Service Requests

Your first task may be to receive jobs from users. Each job will have an AIS service request of some type. A typical AIS service request is illustrated in figure 1-2. In looking over this form, you will notice that it provides you with such information as the following:

- The program name, job number, or task number that is used to reference a particular job application;
- The user's name, department and/or organization, and phone number;
- Where and/or to whom the output is to be sent;
- The desired completion date of the job;
- The computer (machine type) to be used for the job.
- The type of operation to be performed: production, test, assemble, compile, and so on;
- The quantity and type of input media and/or material to be used: magnetic tape, blank checks, and so on; and
- Any special instructions or remarks the user wishes to include.

You will also notice that the lower portion of the AIS service request (see figure 1-2) is reserved for operations use only. This is where you enter the time and date that the job was accepted for processing (lower left-hand corner). The remaining blocks are used by the people in operations to indicate when the job started, when it was completed, along with any significant comments about the job during the time it was run.

If, while reviewing the user's request, you happen to come across a discrepancy or find something that is incomplete or unclear, be sure to bring it to the user's attention. Just remember that throughout the course of your conversation, you are to be tactful and diplomatic. You must always keep in mind that you are representing your command, and the image you project, both personally and professionally, is as important to your job as the work that is being submitted. The key word is communication, NOT confrontation. Once you have accepted the user's request, you make the necessary entries in the job control log.

Job Control Log

A job control log is important, especially when you deal with multiple users. It will be up to you to keep an up-to-date record of all jobs received for processing. A job control log will serve as a continuous point of

AIS SERVICE REQUEST

PROGRAM NAME, JOB, OR TASK # SJC101FT DATE OF REQUEST 3/24/94

From: BARBARA P.

Org. / Ph. # SUPPLY 453-2168

Return to: MR. ROBERTS

BUILDING 3425

SAUFLEY FIELD

Desired Comp. Date

3/30/94

MACHINE TYPE

(Check one)

- ☐ UNIVAC 1100
- ☐ IBM 370
- ☑ BUR 4800
- ☐ Other (specify)

OPERATION TYPE

(Check one or more)

- ☑ Production
- ☐ Assy / Compile
- ☐ Test
- ☐ Other (specify)

THIS FORM IS FORWARDED WITH: SUPPLY INVENTORY RECORDS (1704) CHANGE NOTICE TAPES (3), TAPE #s 126438, 097639, AND 148619

(Type and quantity of input media)

Special inst. / Remarks:

APPLY CHANGE NOTICE TAPES (3) AND INVENTORY RECORDS (1704) INTO DAILY UPDATE. SHOULD ERRORS OCCUR DURING INPUT VALIDATION, NOTIFY BARBARA IMMEDIATELY. OTHERWISE, CONTINUE JOB TO NORMAL EOJ.

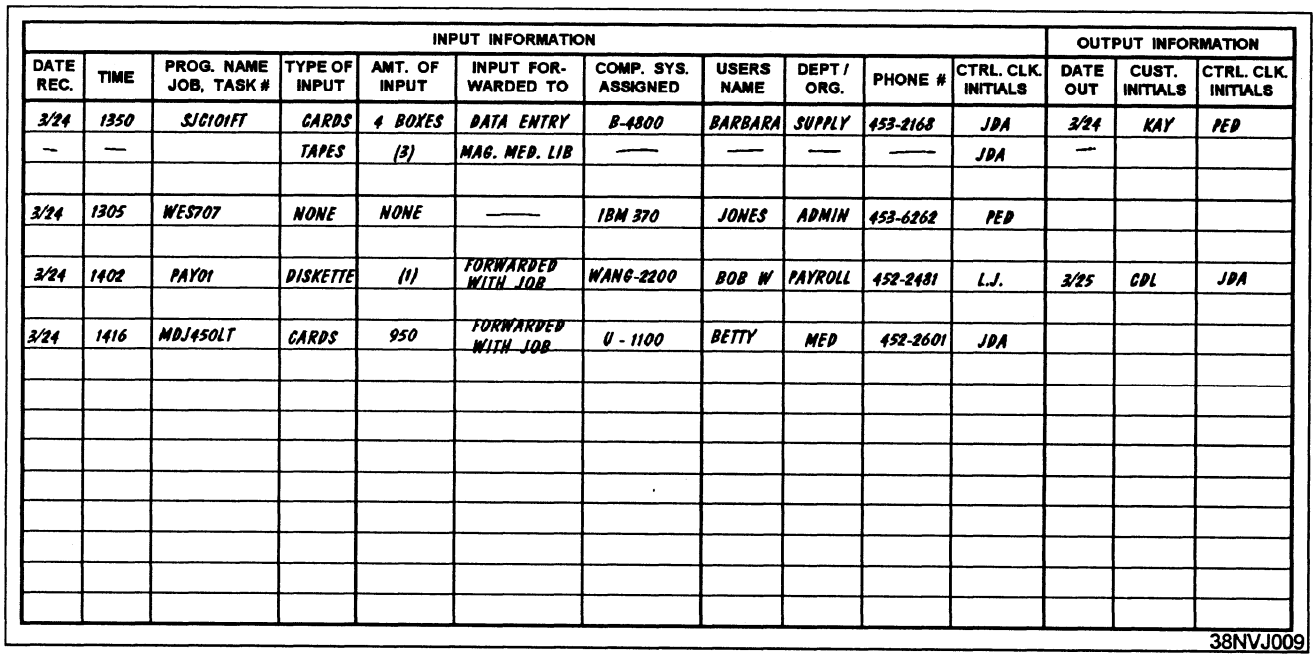
OPERATIONS USE ONLY

Operators comments / Remarks:

Job Accepted (Time – Date)	Job Started (Time – Date)	Job Completed (Time – Date)	Oper. # _____ Mach. # _____
1350 – 3/24/94			

38NVJ008

Figure 1-2.—A typical AIS service request.



INPUT INFORMATION											OUTPUT INFORMATION		
DATE REC.	TIME	PROG. NAME JOB, TASK #	TYPE OF INPUT	AMT. OF INPUT	INPUT FORWARDED TO	COMP. SYS. ASSIGNED	USERS NAME	DEPT / ORG.	PHONE #	CTRL. CLK. INITIALS	DATE OUT	CUST. INITIALS	CTRL. CLK. INITIALS
3/24	1350	SJC101FT	CARDS	4 BOXES	DATA ENTRY	B-4800	BARBARA	SUPPLY	453-2168	JDA	3/24	KAY	PED
—	—		TAPES	(3)	MAG. MED. LIB	—	—	—	—	JDA	—		
3/24	1305	WES707	NONE	NONE	—	IBM 370	JONES	ADMIN	453-6262	PED			
3/24	1402	PAY01	DISKETTE	(1)	FORWARDED WITH JOB	WANG-2200	BOB W	PAYROLL	452-2481	L.J.	3/25	CDL	JDA
3/24	1416	MDJ450LT	CARDS	950	FORWARDED WITH JOB	U - 1100	BETTY	MED	452-2601	JDA			

38NVJ009

Figure 1-3.—Job control log.

reference. Figure 1-3 illustrates a typical layout of input control information.

When you receive a job, make an initial entry in the log. As the job progresses, make additional entries as appropriate. For example, if you send input to data entry to be keyed, record this in the log. In the event a job or its accompanying input becomes side-tracked, misplaced, or lost, you still have a means of tracking down the job or its input. The log can be of great help. It points out such things as when the job was submitted, the disposition of the input media, the location or the computer system to which the job was assigned, the progress (number of steps) the job has already gone through, the type and amount of input submitted, the person who accepted the job, and soon. If you are still unable to locate the missing item, you are able to notify the user. That person's name, organization, and phone number were initial entries in the log.

Job Preparation

To properly prepare the user's job (specifically the input) for processing, you must have a certain amount of information. This information is located in what is called a task folder, job folder, run folder, or run procedure. Do not confuse these with run book, run manual, or run instructions, which provide computer program operating instructions for the operators. The task folder provides you with such things as a run sheet, control parameters, and output requirements.

RUN SHEET.— The run sheet contains the program name or names and the job or task number under which the job (or system) is to be executed or run. In addition, it indicates all of the inputs: magnetic tapes, disks, and diskettes required, depending upon the type of run or possible options the user selected. There could be one or several magnetic tapes and/or disk files needed for the job. You might be required to retrieve them from the media library, or you might just lookup the tape/disk numbers and annotate them on the run sheet.

CONTROL PARAMETERS.— The task folder will also indicate any parameters that are required. These parameters provide application programs with variable information, data elements that change from one run to the next. For example, the type of run requested: (D)aily, (W)eekly, (M)onthly, (Y)early, (E)dit input only, and so on, or the entering of a date. You maybe required to key in one or several of these parameters, depending upon the complexity of the system.

OUTPUT REQUIREMENTS.— The task folder and/or the computer run sheet show you all of the output products: magnetic tapes/disks, and special forms that are produced during the running of the job or system. As an I/O control clerk, you maybe tasked to provide the computer operators with the correct number of blank, handwritten, or preprinted output tape/disk labels and ensure a sufficient supply of tapes, disks, paper, and special forms are on hand before the job or system is scheduled to be run.

Job Monitoring

Although we would like to believe all jobs run without error, there are occasions when a program

prematurely or abnormally terminates. It does not process to normal end of job (EOJ). When this occurs, the operator is expected to take whatever corrective actions are necessary to get the job going again. More often than not, the operator is able to recover a job by recreating a tape/disk file, moving the file to another device, or possibly cleaning the read/write mechanisms of the device prior to rerun. But, there are times when the operator will notify you (the I/O control clerk) to assist in correcting the problem. Such would be the case when the input parameters are in error, the user's input is bad, or the job aborted because of an unrecoverable program error. If this happens, you maybe responsible for collecting all the data, both input and output, along with any memory dumps, and forwarding them all to the programmer.

During the recovery phase of an operation, the operator may need you to provide certain input parameters or tape/disk files before the job can be executed. Because of time constraints, a job that abnormally terminates may have to be rescheduled. If so, you may be responsible for seeing to it that the job gets rescheduled and that the user is notified of any job delay. We could go on and on, but by now you are beginning to get the picture. These examples are just a few of the many things that can get in the way of achieving a normal EOJ. We bring them to your attention to make you aware of the types of problems that can and do arise, and the manner in which you are to respond. Hopefully, you now know and are aware that monitoring a job means more than just calling up the operator to see how the job is progressing. It means you must oversee the job to its completion, doing whatever is necessary to help keep the job (or system) on track.

Output Products

Output from computer processing—The work that has been completed—may take the form of a printed document, magnetic tape, or magnetic disk or diskette. In all cases, both you and the computer operator are responsible for ensuring that all completed jobs run successfully. In addition, you are responsible for identifying and coordinating the various outputs for each job, and for initiating their correct distribution.

To determine whether a job (or system) ran successfully (to a normal EOJ) and that all processing steps were properly performed, you may have to review the computer console printout. This printout indicates such things as the number of input records read, the various input files updated, all error conditions (error messages) that the operator encountered during the run and the resulting actions taken, the various output files created, and so on.

In the majority of cases, the computer console printout will provide you with the answers you are looking for when it comes to reconciling processing discrepancies. For example, it will inform you of the reasons certain output products—tapes, diskettes, or report listings—were not produced. Possibly the operator selected an incorrect program option, or the input parameters were incorrect or incomplete before starting the job. In short, you are responsible and also accountable for every job you work on, from the time it is submitted by the user until its delivery back to the user.

When checking the user's output, you should once again refer to the run sheet and/or task folder to verify that all items requested were, in fact, produced. If the output is in the form of magnetic tape, disk, or diskette, be sure it is labeled properly, given the proper classification, and it is on the appropriate media (magnetic media that has been designated for mail-out or distribution only).

When checking reports, make sure they were run on the proper forms (size and type), that no pages are missing and the correct number of copies were printed, and that all print is legible and lined up properly.

Once the output is checked, you then package each completed copy of the report, along with any other output products and the original input, place it in the proper pickup area, and log the job out in the job control log. You may need to notify the user when the job is ready.

If, during the course of checking over the user's output, you happen to come across something unusual or you find an error, by all means, pull (reject) the job immediately, bring it to the attention of your superior, and notify the user of the delay. Even at this late stage, it is better to reject a job to connect any problems or discrepancies rather than to release it, only to have it returned for rerun later.

USER SUPPORT

The term *user support* covers a broad range of duties. They include answering inquiries from users, providing logistical support, and processing trouble reports.

User Inquiries

Normal inquiries from users include system status, job status, and reporting trouble. It is the job of the technician to answer these questions promptly and accurately. A user might ask:

- Why is the system slow?

- What is the status of a particular job?
- What step is it in?
- Has it printed out yet?
- Do I have a problem with my terminal?

Logistical Support

The most common user support you will deal with is logistical support. This will include the need for new or different equipment to meet the command's mission or current equipment that needs corrective maintenance, or scheduling preventive maintenance. Forward this type of user support to the division chief or the division officer, since it requires the relocation or the acquisition of equipment.

Trouble Calls

As the technician, you will be receiving and responding to trouble calls. When the user calls to submit a trouble call, remember to get all the required information:

- User's name;
- Type of trouble encountered;
- Date and time; and
- Job being done when the trouble started.

The preceding is only an example of what might be included on the trouble report at your command. Your command will have the reporting procedures for submitting trouble reports, with an example of a trouble report. Each command has a specific trouble call format and a tracking procedure.

CUSTOMER LIAISON

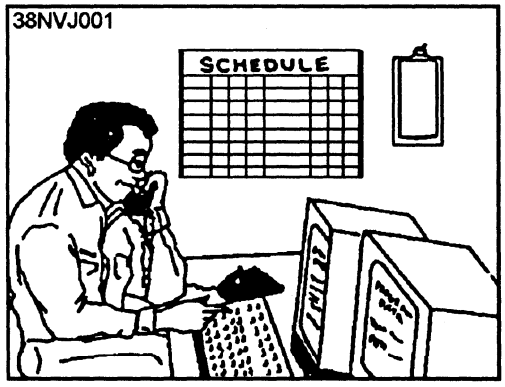
When involved with or communicating with the user (customer), you must use tact and diplomacy. You must be able to understand and resolve the requests of the customer. You will also have to deal with discrepancies and explain problems to customers. You must be able to independently recognize and resolve discrepancies and be knowledgeable enough to know when you can resolve a discrepancy and when to refer complex problems to your supervisor or leading chief.

MANAGING PRODUCTION

Once you become a shift supervisor, you will be responsible for managing the scheduling and operation of all production activities associated with computer processing within your shift. You will monitor the workflow and make adjustments to meet changing requirements.

During your work shift, one of your many jobs will be to monitor job/production status on a regular basis to determine if there is any actual or potential slippage in the schedule. It will be your job to balance operations resources and optimize workflow. There will be times when you must make adjustments in the sequence of work (within the constraints of the overall schedule) to optimize productivity. In computer operations, you must be able to examine problems that have occurred during production and initiate corrective action within operations or with the users.

THE SCHEDULING ENVIRONMENT AND REQUIREMENTS



Schedulers and production control coordinators are responsible for coordinating the work efforts of many people. They prepare, distribute, and maintain production schedules for their AIS facility or data center. They analyze job requirements (old and new) to determine the impact each job has on production resources. They also inform the LPO or division chief when scheduling requirements will exceed computer system resources. In short, schedulers act as coordinators from the time a request is received until a job is successfully completed. The scheduler is responsible for keeping the AIS facility's assembly line running as smoothly and efflciently as possible. Schedulers ensure that jobs are scheduled and entered into the production job stream at the proper time. They also ensure that all necessary resources are available to maintain a constant workflow throughout the AIS facility.

PEOPLE, PLACES, and THINGS are the important factors of a scheduler's job. The first factor is PEOPLE. You must learn to deal with various personalities. The second factor is PLACES. You have to learn what goes on in other fictional work areas. The third factor is THINGS. You have to cope with run times, deadlines, computer hardware and software

malfunctions, problems with production programs, and TIME itself (that 24-hour period in which you are to schedule as much production work as possible).

THE SCHEDULING ENVIRONMENT

How difficult is it to prepare a schedule? you might ask. That depends on the size and complexity of your data processing installation in terms of hardware, software, and support personnel. You must consider many things when preparing a schedule. As a start, you have to ask yourself the following questions:

- What types of jobs are to be processed?
- In what processing environment will the jobs run—real-time? online? batch?
- What special-handling requirements are there, if any?
- What amount of work is to be processed (workload)?

As scheduler, you will be responsible for:

- Preparing and maintaining established schedules for various time periods: daily, weekly, and monthly;
- Reviewing and acting on all types of AIS service requests as they are submitted to you;
- Distributing production schedules to various work areas within your AIS facility;
- Organizing data processing priorities for both scheduled and nonscheduled work;
- Entering jobs into the production job stream to achieve maximum use of computer resources;
- Tracking work in progress to ensure everything is running according to schedule;
- Analyzing problems in connection with production jobs and adjusting computer processing schedules to use whatever time is available until problems can be corrected and a rerun can be initiated;
- Maintaining accurate logs and adhering to administrative reporting requirements; and
- Determining the accuracy of schedules based on reviewing production results.

How you go about scheduling work on the computer system will depend on two factors. The first factor deals with how the system is configured. You must consider the number of processors and peripheral devices available and how they interconnect. The second factor deals with the operating mode of the computer. The operating mode may be batch, online, real-time, time sharing, multiprogramming, multiprocessing, teleprocessing, networking, or any combination of these. Having knowledge of the different operating modes will help you understand the operating environment in which you will be working. This knowledge will help you understand how to go about scheduling work for the system.

THE JOB OF SCHEDULER

The job of scheduler, or production control coordinator as it is sometimes called, requires you to have specific knowledge and skills if you are to effectively schedule the computer and the other related activities that revolve around it. You must have a good working knowledge of AIS concepts and be thoroughly familiar with the operation of your facility's computer system(s)—the actual hardware components themselves. You also need to know how the operating system in use works, what applications and production jobs you are to schedule, the time it takes to run them, how to make up job streams using system control language (SCL) statements, and so on.

One of your primary jobs will be to keep production schedules up-to-date and as accurate and complete as possible. In addition to making up production schedules for computer processing, you must be equally concerned with two other factors: **precomputer processing** and **postcomputer processing.**

Precomputer processing includes ensuring all inputs are received on time according to prearranged schedules. Postcomputer processing includes ensuring output products are complete, accurate, and delivered to the user when promised. Too often these areas are either overlooked or forgotten, because our interest is generally focused on the computer. We can easily overload or underload precomputer and postcomputer resources. This will have the same effect as overloading or underloading the computer—either user service deteriorates or AIS services are underused. For **TOTAL** AIS scheduling to be achieved, YOU must consider all of the fictional work areas in the assembly line, especially the end users. All are affected by the scheduling process, and because of this, you must give each work area proper consideration.

Having working knowledge and experience in the fictional areas for which you will prepare schedules will also help you. As scheduler, you will be putting

together information from several sources: I/O control, data entry, and the magnetic media library.

Depending upon how your AIS facility is structured, your operational requirements will include tasks, duties, and functions as follows:

- Receive user job requests.
- Analyze production requirements.
- Assign job/run control numbers.
- Maintain accurate logs.
- Carry out administrative reporting requirements.
- Prepare production schedules.
- Write SCL statements.
- Make up job streams for production runs.
- Maintain and revise production schedules.
- Distribute production schedules.
- Monitor production.
- Know how jobs interface.
- Be able to read console run sheets and logs.
- Know the capabilities and capacities of the computer systems.
- Know the files in use and how to reconstruct them.
- Know how to readjust schedules.
- Know the time it takes to run each production job.

As scheduler, you will work on your own with only minimal supervision. To be effective, you will need more than a good working knowledge of your facility's hardware components, data processing concepts, operating systems, and system control languages. You must be able to:

- Work well with other people;
- Demonstrate tact and diplomacy;
- Use sound judgment;
- Be logical, systematic, and persuasive;
- Demonstrate analytical ability;
- Be a good communicator (speaking, listening, and writing); and
- Be responsive to users' needs.

The job of a scheduler is a high-visibility position. You will be responsible not only for the flow of work throughout the AIS facility but also for the amount of work that will be accomplished within an allocated period of time.

AIS WORKFLOW ANALYSIS

Every AIS facility is site unique regarding the types of hardware and operating system (OS) software in use. However, every site does have a formal or informal workload structure that encompasses all of the AIS fictional work areas and the users. Figure 1-4 illustrates a typical AIS facility's workflow structure. This particular site operates in a multiprogramming environment and handles batch, online batch, and real-time processing. Study this figure for a moment. You will see how the work flows in, and about, and out of the AIS facility. You will see how you, as a scheduler, fit into the picture.

In looking at figure 1-4, you will notice this AIS facility is composed of five fictional work areas:

- Production Control—Scheduling, I/O Control, Quality Control;
- Data Entry;
- Computer Operations;
- Media Library; and
- Technical Support.

Each functional work area is responsible for specific segments of the workflow. How they work together and with you, as the scheduler, will determine if your job is easier or more difficult. Learn what they do. The next paragraphs will give you a basic understanding of their responsibilities and their interactions with other work areas.

PRODUCTION CONTROL personnel act as liaison between the AIS facility and the user community. The division chief and LPO normally deal with users during the initial scheduling phase. They will assist scheduling by ironing out any problems early in the scheduling phase. When necessary, they will also work with the users to adjust data flow and output schedules based on user and production requirements.

SCHEDULING personnel make production commitments for the AIS facility to meet user requirements. They provide processing schedules to coordinate inputs and outputs between I/O control, data

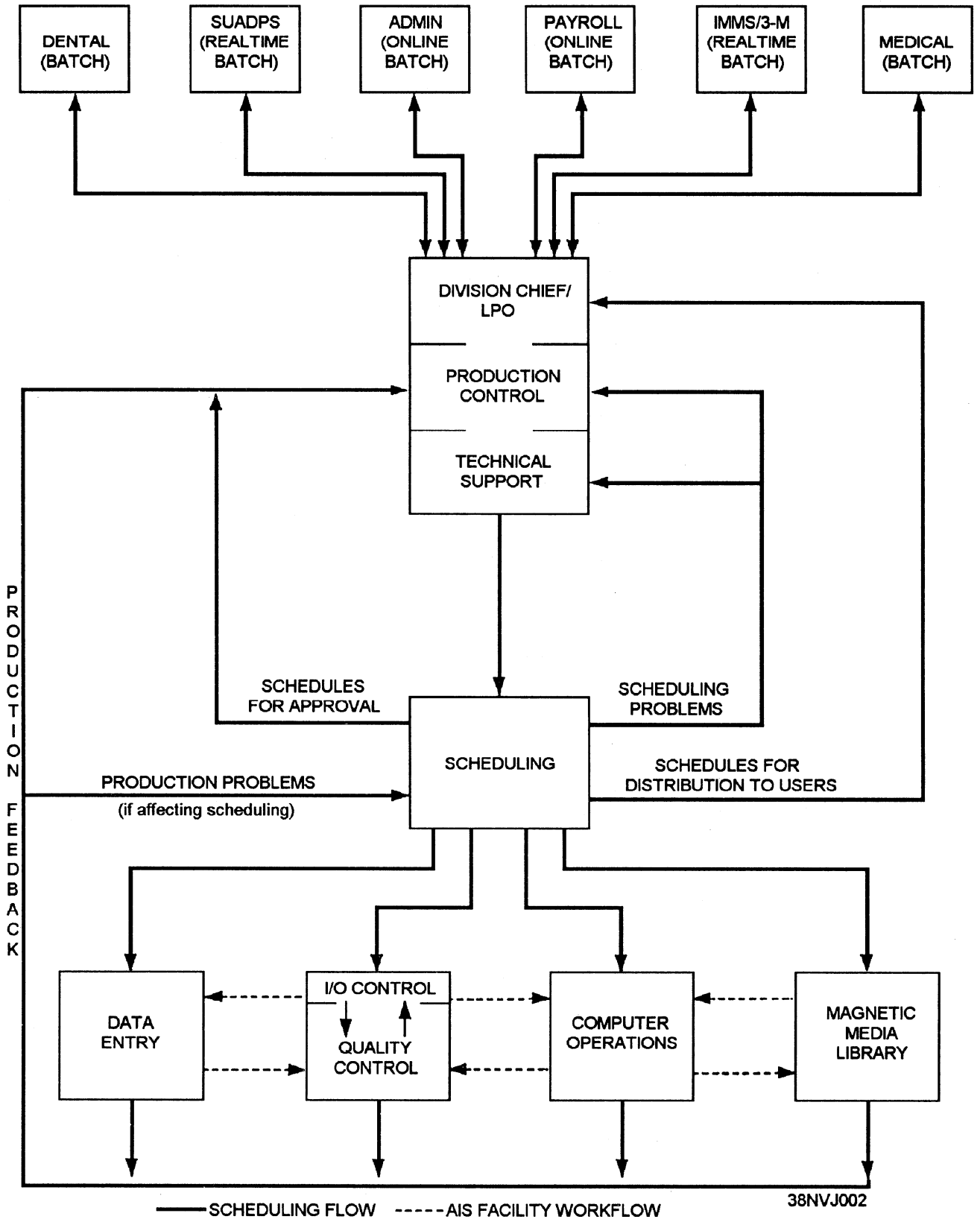


Figure 1-4.—AIS facility workflow structure.

entry, computer operations, and the magnetic media library.

I/O CONTROL personnel handle all incoming work for AIS services along with all types of input media from the user. Some of these inputs are source documents, magnetic tape, and diskettes. I/O control personnel perform the following tasks:

- Count, verify, edit, and total all source documents received;
- Check that the amount of input data is approximately the same amount as was indicated in the production schedule;
- Verify all incoming work for accuracy and legibility;
- Log all inputs received in various input/output control logs;
- Coordinate the receipt of late submissions with users and scheduling;
- Forward source documents to data entry and computer inputs to either computer operations or the media library depending on when the job is scheduled;
- Receive output products from quality control; process, log, and package output products; and ensure proper and timely delivery to users.

QUALITY CONTROL personnel review all completed output products from data entry and computer operations to determine their accuracy and completeness before releasing them to I/O control personnel for further processing and distribution. They forward incomplete or incorrect jobs to scheduling or technical support for further investigation.

DATA ENTRY personnel convert source documents into machine-readable form using some type of key-driven (terminal) device if this is not done by the user. They accept source documents, key-enter and verify all inputs, and return completed data to quality control so it can be checked for completeness and accuracy before turning it back over to I/O control to be submitted with the job.

COMPUTER OPERATIONS personnel operate the computer and associated peripheral devices in accordance with authorized schedules. They receive inputs and associated run instructions from I/O control, update schedules as the work is completed, forward output products to quality control, and transfer magnetic media to the library for further handling and processing.

MEDIA LIBRARY personnel check in/out tapes, disks, diskettes, and documentation to computer operations personnel. They also condition, clean, retire, store, and transfer magnetic media to off-site storage and other outside activities.

TECHNICAL SUPPORT personnel provide scheduling and production control with technical support, as needed, to resolve production problems. They examine problems that occur during production to determine if errors were caused by hardware or system/applications software. Then, they initiate corrective action with computer operations and/or scheduling.

By charting all AIS facility functions and defining their interrelationships, you, as scheduler, are able to create a workflow diagram for your particular scheduling environment. It will help you to decide which functions and fictional areas require scheduling and which do not. Now that you have some idea of how the work flows in, and about, and out of the AIS facility, let's see how you, as a scheduler, fit into the picture.

Normally, the users get together with the division chief, LPO, and yourself (as scheduler) to make their requests for AIS services known for the upcoming month(s). This initial scheduling phase is known as the *planning phase* or *forecasting phase.* By knowing these workload demands early, more time is available to determine where excessive demands and inadequate demands are being made on resources. To put it another way, the forecasting phase allows everyone to see where there may be an overloading or underloading of AIS resources.

As the users go about presenting their daily, weekly, and monthly requirements, you will be busy incorporating their requirements into the production schedule. During the forecasting phase, you must remember to set aside whatever time is needed for file and computer maintenance. You should pay particular attention to those out-of-the-ordinary and one-time requests that tend to pop up. These, too, must be accommodated in the schedule. When given a new job where there are no previous production statistics, ask the user for a rough time estimate of how long the job may run. Ask if there will be input data, and if so, will it require data entry services. Know how many and what resources the job will use. Know the environment in which the job will run—online, batch, or real-time. You will want to keep a close eye on new jobs.

Using previous schedules and scheduling procedures as a guideline, you can begin to prepare

(plan) a rough schedule. When scheduling old jobs, you will have expience and history to follow. Knowing what resources (hardware, software, and personnel) your AIS facility has available will help you see where the peaks (overloading) and valleys (underloading) are in the schedule. It will be your job to take the resources, the time available, the estimated run times, the time jobs must be started and completed, and whatever other information is needed to establish a meaningful and workable schedule with the best job mix possible. You will prioritize and plan. Once you have ironed out all the wrinkles and prepared a smooth schedule, you will submit it up the chain of command for approval. Once approved, you will distribute the schedules to the various functional work areas.

THE BENEFITS OF SCHEDULING

What are some of the benefits of having a schedule/ scheduling system in place? One answer is PREDICT-ABILITY. A scheduling system makes everyone's job easier by adding predictability to the AIS environment. To your superiors, it provides a means of holding down costs through better use of personnel and equipment. Other possible benefits of scheduling areas follows:

- Effective use of all AIS resources;
- Increased throughput;
- Decreased turnaround time;
- User deadlines met;
- Users made responsible for providing input on schedule;
- Improved communications with users;
- Avoidance of overloading and underuse of resources;
- Job delays more readily apparent;
- Documentation of scheduling deviations and their causes;
- Reduced confusion within the AIS facility;
- Better use of multiprogramming capabilities;
- AIS facility able to review its own effectiveness;
- Predictability of the effects of an increased workload; and
- Predictability of future equipment and personnel needs.

All of these benefits can be achieved through an effective scheduling system.

THE SCHEDULING PROCESS

The scheduling process has three moving parts: you, the information, and the method. Let's look at each.

THE SCHEDULER

As scheduler, you must be well organized. Scheduling jobs through the various work areas within your AIS facility is much like scheduling the events of your own personal day-to-day life, except it's a lot more technical and involved. You set aside predetermined amounts of time to do certain things. Call it "a things-to-do list" if you will.

It would be nice if your things-to-do list consisted of nothing more than having to accept incoming requests from the users, finding holes to plug their jobs into the schedule, and waiting for the jobs to show up on the completed list. If that were the case, your things-to-do list would be relatively small and seemingly uncomplicated. If your AIS facility has such an abundance of resources that any demands made by the users can be easily met, then your facility is probably wasting resources and incurring more expenses than it should. This is probably not the case. To the contrary, your command will probably have just enough resources or too few.

As scheduler, you must decide which jobs to process first, second, third, and so on. Which jobs can be run together? You need to determine the job mix. How big are the jobs in terms of memory use? What resources do they use-disk drives, tape drives, printer, and so on? How long will each job run? In what environment must each job be run?

Under ideal conditions, you can work through your things-to-do list in a relatively short period of time and come up with a workable schedule. In reality, however, things do not necessarily go according to plan or, rather, according to schedule. Equipment, other people, and outside influences are all problem areas.

A lack of productivity and missed deadlines can be caused by unexpected problems, such as:

- Late submission of input from the user;
- Waiting for data entry to complete a job step;
- Having to locate a missing file in the library;
- Job stream parameters entered into the system incorrectly.

You may face any number of these and other situations each day. You should have a backup or contingency plan in the event you lose a piece of hardware. For example, if the fastest printer is down, will the user be satisfied with one printed copy now and the remaining copies printed tomorrow? Or is there another AIS facility in your immediate area that will let you use its printer? It will be your job to prepare the most realistic schedule you can, and then be ready to adjust it. What tools will you have to help you prepare the schedules? What information will you need? What methods can you use? In the following section, we talk about the types of information you will need to prepare a schedule. Then we explore a few of the scheduling methods you might use.

INFORMATION NEEDS

Regardless of the scheduling method used, you will need to know specific types of information. Some information is *job-related;* that is, information about the resources, media, and time needed for a particular job. Some information is *AIS facility-related;* for example, workload, anticipated resource changes, number of operators available, the system capabilities and capacities, and so on. You will need to consider both. Let's look at the job-related and AIS facility-related areas in a little more depth.

One of the most apparent pieces of job-related information is that every job has resource requirements. These requirements vary considerably from one job to the next. One job may require 125K of memory with no other peripheral devices except a printer for output. Another job may require four tape drives, two disk drives, a printer, and only 40K of memory. But a job's resources cannot be looked at in these terms alone. Can you recall the terms PREcomputer and POSTcomputer processing? All AIS facility resources must be considered. You must consider data entry functions, job setup functions, and output control functions. Overloading data entry can delay jobs, causing them to be assembled for computer processing later than scheduled. Suppose I/O control is overloaded. What difference would it make if jobs were processed and completed as scheduled? They would only be delayed because work is backed up or personnel are not available. Overutilization of resources affects service. Underutilization of resources is expensive and wasteful. The balance will be up to you and the efficiency of your schedule.

Another piece of job-related information to consider is *processing time.* To set aside a sufficient amount of time for processing, you must know how long a job will reside in memory. Processing time is normally estimated for a multiprogramming environment since most computers today process programs/data in this fashion, and job mix affects the overall processing time for a job.

Let's assume you have a static workload with no jobs being added to or deleted from the schedule. Even under these conditions, you can expect job processing to deviate from the schedule. Why? you might ask. The reasons for this are the uncertainty about job processing time and disrupted processing. Take, for example, a job that normally has a processing time of 45 minutes. Today, because of a large increase in input, the job processing time is 1 hour, thus delaying all the following jobs by 15 minutes. This is unavoidable and must be expected. The same is true of disrupted processing, whether it is hardware failure or software problems. One way to avoid these delays is to include a specified amount of buffer time in your schedule. You might add a safety factor of 10 percent to the expected processing time. In our previous example where processing time increased from 45 minutes to 1 hour, a buffer time of 10 percent would only give you an additional 4.5 minutes of processing time. This would still have been inadequate. However, since all the following jobs also have buffer time built into their scheduled processing time, the job overrun should not be that critical for meeting the overall schedule of a shift.

Another piece of job-related information to consider applies to multiprogramming environments. The challenge here is to combine as many jobs as possible so that each resource is used to its maximum. In a nonmultiprogramming environment, you have no problem in scheduling jobs because you can process only one job at a time. However, resources are underutilized, and that's a fact you must live with. This is a direct result of having all resources dedicated to one computer, even when they are not needed. On the other hand, multiprogramming allows you to execute several jobs at the same time using as many resources as possible. The difficulty of manually preparing such a schedule for a system that runs in a multiprogramming environment is in trying to obtain a job mix that makes the best use of most resources without bogging down the entire computer system.

Figure 1-5 gives you some idea of how main storage and peripherals can be fully utilized as a result of the proper job mix. It shows where the jobs are in memory, and what tapes and disk drives are used by each job. It also shows information about printing and printers. It

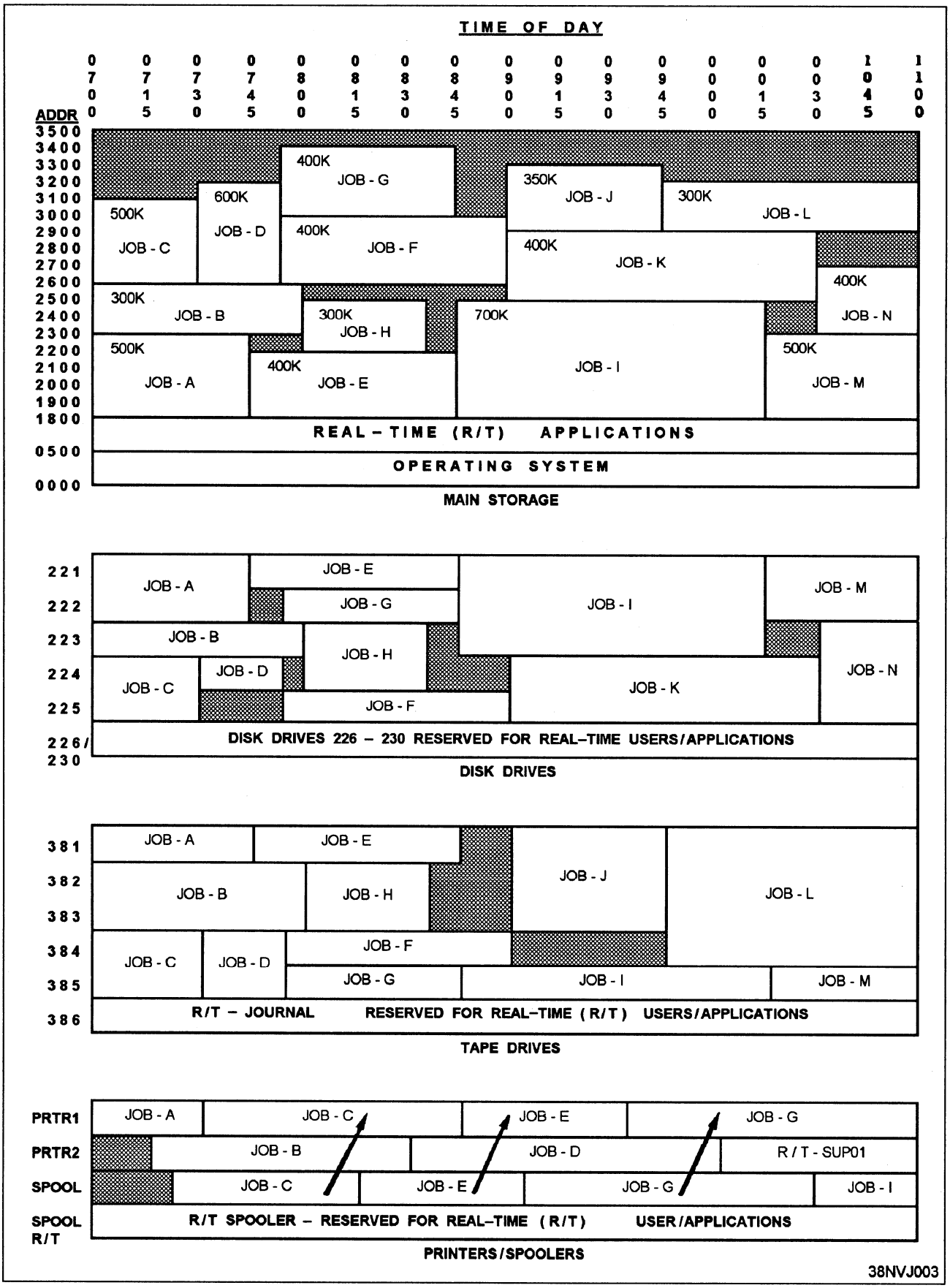


Figure 1-5.—Resource utilization in a multiprogramming environment.

is difficult to obtain an optimum job mix using manual scheduling techniques, but it can be done. Most often, the solution to obtaining maximum throughput in a multiprogramming environment (on a continuous 24-hour basis) is to use one of the more sophisticated automated scheduling packages. These packages have all of the considerations we have been discussing programmed into the software.

Another piece of job-related information to consider is *job dependencies.* Most AIS facilities process both single-program jobs and multiprogram systems. Examples of multiprogram systems are the supply and 3-M systems. These systems consist of many programs that are normally executed as separate job steps within a system. Or, the programs may be processed as separate jobs that must be processed in a specific sequence. Therefore, you must know their proper sequence. It would be foolish to execute a job that prints the output of an updated file that had yet to be updated. It should be just as obvious if a job abnormally terminates that all jobs following it must be canceled and rescheduled, allowing sufficient time for the terminated job to be rerun. Canceling and rescheduling dependent jobs may seem like an easy task to perform. However, in reality, it can become a complex and difficult operation.

And finally, we have priorities and deadlines to consider. Some scheduling methods place primary importance on priority. Each job is assigned a priority, and the jobs are processed according to the highest-priority job that can be scheduled based on available resources. Priority scheduling is often used in automated scheduling systems. Some scheduling methods place primary importance on deadlines, processing jobs according to the earliest deadline or sometimes latest deadline. When you prepare a schedule, remember to take into account job requirements that include the following:

- Data entry;
- Job setup and output control functions;
- Computer processing time;
- Resource requirements;
- Operating environment;
- Job dependencies;
- Job priorities; and
- Deadlines.

Now that we have covered job-related information, we will discuss AIS facility-related areas and how these can affect your production schedule.

You may recall that to prepare an effective schedule, you must know your AIS facility's resources: how work comes into, flows through, and leaves your facility; the capabilities and capacities of your system; and workload demands on the system. As a scheduler, your goal is to match resource capacities (people, places, and things) to workload demands while satisfying user deadlines and priorities. This is often difficult to do, especially when resource capacities vary because of hardware failures, specific shift requirements, personnel on leave, and unpredictable user demands. Your workload can exceed capacity, which has a direct effect on service. Or, the capacity can exceed the workload. This leaves AIS resources underutilized. So how do you reach a happy medium? you might ask. You do it by ensuring that the workload demands put upon the AIS facility's resources are balanced as much as possible and that the total resources available are kept as close to the maximum capacity as possible.

The effective use of resources has a lot to do with how you prepare a schedule. However, other things affect scheduling effectiveness. One thing that disrupts schedules is the late receipt of input from the users. This often results in a lot of hectic activity. Data entry, possibly I/O control, and computer operations have to try to meet original deadline commitments. If they cannot, you, as the scheduler, have to reschedule jobs, while dissatisfied users complain because their jobs are not out on time.

But you say the user has no right to complain? You are right. Often, the users do not realize they are the cause of the delays. So what can you do? Educate them! Inform the users of the effects late input submissions have on the schedule. They sometimes do not realize how long it takes to prepare their input. All jobs scheduled should have an established input receipt time. When scheduling, include in your schedule sufficient buffer time between scheduled receipt time and actual due time. And last, but not least, report scheduling deviations and their causes to your superiors. In this way, the process can be reviewed and improved.

Something else you have to consider in connection with scheduling effectiveness is your ability to reschedule quickly. You must be prepared to make adjustments to schedules. You will have to contend with power outages, corrective maintenance, deadlines or priority changes, special job requests, and so on. You must also consider processing delays. Rejected transactions may have to be reentered before a priority

job can continue. An unreadable tape or disk file may have to be recreated. Errors in SCL statements in the job stream may have to be corrected. The most serious delays usually result from abnormally terminated jobs and hardware failures. Regardless of what the situation may be, you must be prepared to readjust schedules as quickly as possible with a minimum of disruption.

PRODUCTION SCHEDULING

The AIS facility is tasked with the responsibility of providing computer support to the command. This includes support to medical/dental, supply, administration, financial, and maintenance. Each of these areas will have a subsystem coordinator assigned to work with you on monthly schedule requirements and on processing problems. You will also prepare daily workload schedules.

MONTHLY PRODUCTION SCHEDULE DEVELOPMENT

As the AIS manager, you will be responsible for developing and distributing a monthly AIS operations schedule. You have used monthly schedules, but you may never have given much thought as to what it takes to develop one.

To develop the monthly schedule, you must know the requirements of all the application systems/jobs to be run during the month. Many production jobs are run on a cyclic basis—daily; Monday, Wednesday, and Friday; weekly; monthly; quarterly; semiannually; or annually. Be sure time is included for testing, planned maintenance, file maintenance, and backup procedures. For systems with online users, be sure to provide ample capacity and time.

Schedule Review

Once you have developed the monthly schedule, you must ensure that the schedule is adequate and meets the requirements. To do this, you will see that the proposed monthly production schedule is distributed to the appropriate subsystem coordinators for their review. Before the end of the current month, the subsystem coordinators are to return the monthly schedule with their concurrences or changes and recommendations back to you for screening. You will screen it to ensure they have not overscheduled any day, and that there will be enough time for system backups and planned maintenance. The screening process should include a review by the production control coordinator, who looks for any specific input/output requirements. For example, special forms may have to be ordered. This must be done early enough to have the forms when the job is to be run. After screening the changes and recommendations and making any adjustments needed, have a smooth copy of the schedule prepared and distributed to all subsystem coordinators and the department head before the beginning of the month to which the schedule applies. Figure 1-6 is an example of part of a monthly production schedule.

Month _____ Year_____

Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1 Suadps Monthly	2 Suadps Monthly	3 Weekly Saves
4 PMS	5 AV3M NAVFLRS	6 MSSL MRL	7 Dummy Monthly MSF	8 AV3M NAVFLRS	9 Dummy Monthly MSF	10 Weekly Saves
11 PMS	12 AV3M NAVFLRS	13 Dummy Monthly MSF	14 Stock Release	15 AV3M NAVFLRS	16 Dummy Monthly MSF	17 Weekly Saves
18	19	20	21	22	23	24

Figure 1-6.—Part of a monthly production schedule.

Effects on Monthly Schedules

After the monthly schedule is completed and approved, there will always be times when it has to be changed. The subsystem coordinators are responsible for adjusting their schedule and for submitting the schedule changes to the AIS facility. Some of the things that will cause the schedule to be changed are as follows:

- **System/program errors.** Jobs may abort because of system or program processing errors. The operator will get an error message or an indication on the system console. This may require the operator to reboot the system, recreate an input file, or rerun a job. The operator will annotate the run sheet describing the problem. The abort code will be the key to determining what caused the problem.
- **Software testing.** You will schedule an amount of time for software testing based on your best estimate. No matter how much time you allow for software testing, it will never seem to be enough. Problems seem to arise every time you start to test a new software system. These include the system going down, the system hanging up, the system entering a loop, or a syntax error occurring that the programmers missed.
- **New/changed requirements.** There will be times when jobs are added to the schedule to meet special needs. Examples are budget cuts, extra money at the end of the month, requisitions, tracking, and assist visit preparation.
- **Job conflicts.** A job with a high priority maybe submitted late.
- **Input files not available.** Sometimes there will be a delay in receiving the input files for a job.

Whatever the problem, it will be the production control coordinator's job, with your approval, to adjust the schedule to accommodate the changes required.

WORKLOAD SCHEDULE DEVELOPMENT

When we talk about workload schedules, we are referring to how to set up the daily work schedule in an AIS facility. These are the daily adjustments to the monthly production schedule and how they affect personnel requirements and staffing. This is an internal schedule that you will prepare for the AIS facility. The format varies among facilities; there is no wrong or right format. Normally, we break the day into three shifts—days, eves, and mids. The day shift is responsible for testing. The eve shift is responsible for production. The mid shift is responsible for finishing production and doing the nightly saves.

You will have to develop the workload schedule by reviewing the monthly schedule and combining it with any newer information. The input/output requirements will have to be reviewed, and you will need to be ready to make changes to the schedule based on unforeseen events.

System Input/Output Requirements

Before a job is started, certain input and output requirements must be met. The I/O control clerk must review the production workload schedule to see which job is to be run. Then the clerk must look at the job run folder to make sure that all the input files are available and all the necessary output media is readily available.

- **Input requirements.** If the job requires tapes or disk files as input, the I/O control clerk will check with the media librarian to see if these files are ready and available. And, if they are not ready, when they will be available for the job. In some cases, it maybe necessary to reschedule a job while waiting for the input.
- **Output requirements.** The job may require special forms or multipart paper to be printed. The I/O control clerk will check the job run folder to see if the job will require any special forms and then check to see that they are available. The production control coordinator will have looked at the requirements when the monthly schedule was developed to allow enough time to order the forms. The job may produce output tapes or diskettes, requiring the I/O control clerk to check with the media librarian to make sure enough scratch tapes and blank diskettes are available for the job.

Effects on Workload Schedules

On any given day or shift, almost anything can go wrong. A job may abort. A tape may not read. User requirements may change. A high-priority job maybe submitted. Personnel may be called off the job to do something else. This means there will be times when you must change the way work is to be completed

during the day. For example, to stay on schedule during monthly, quarterly, or yearly processing, production work will have to be run during the day shift. You may also have to have additional saves run in association with monthly, quarterly, or yearly processing. Another example is as you are preparing to load a software update, you might have special saves run during another shift. This will ensure that the data is backed up and a good copy of the software is available if the update does not work properly. You may also have to reschedule some of the production work.

Anytime the normal work schedule is changed, it may affect the online users by slowing the system response time or causing the system to be unavailable to the users. Care must be taken when the schedule is to be changed. Try to cause the minimum interruption to online users, and do keep them notified of the changes.

PRODUCTION PROCESSING

During production processing, the I/O control clerk, production control coordinator, and operators will monitor the schedule and the jobs to see that the work is being accomplished as planned. When problems arise, as they will, you may need to become involved. You may be involved in determining the cause of the problem and in working with the user to solve the problem. The common causes of problems are application program processing errors and system downtime.

Users must be informed concerning any production problems pertaining to their jobs. When you talk to the users, you must know which job had the problem, what the problem was, and what, if anything, AIS can door did do to correct the problem. Besides notifying the user of production problems, you will be required to notify them of system downtime or nonavailability. Setting up procedures for the operator and the production controller to follow will help in solving problems and in communications with users.

For online users, the subsystem coordinators are the most qualified and highly trained individuals on their particular subsystem and should be assisting users with processing problems. This does not eliminate the need for the operators to become knowledgeable in the workings of each subsystem, since they normally are called first when a problem occurs. You will need to examine any production problems that occur and work with the shift supervisor and/or production control coordinator to be sure proper corrective action was taken.

APPLICATION PROGRAM PROCESSING ERRORS

To determine the causes of application program errors, you have two areas of concern—hardware and software. Let's look at some of the most common causes in each of these areas.

Hardware Problems

With respect to the hardware, not only each specific piece of equipment is a possible cause of a problem, but you also have external environmental concerns.

Some of the most frequent hardware problems are:

- Head crash;
- Tape drive damage to a tape; and
- Tape read/write errors.

If tape read/write errors cannot be conected by cleaning the read/write heads, a maintenance technician should be called. For head crashes and tape drive damage, a maintenance technician should always be called.

The most common external environmental problems are:

- Loss of power;
- Voltage spikes; and
- Loss of air conditioning.

What action should be taken will depend on the damage done. The operator may be able to recover the job completely by rebooting and restarting the job. If the data files have been corrupted, the operator may need assistance from the user and/or the media librarian.

Software Problems

Examples of the common software problems are:

- Wrong file specified;
- Program entered a loop; and
- File not available.

The preceding is only a very brief list of possible problems. There are too many different causes to list in

this manual because of the number of different application software programs being used.

To correct software-related problems, the operator must refer to the job run folder and the program operator manual for the corrective action to take. Your operators will have predefined steps to follow when researching the cause of the error in the specific program operator's manual. The operator manual explains the steps to follow in connecting the problem and any restart points. The job run folder will contain the name and phone number of the person to contact if the problem cannot be easily corrected.

SYSTEM DOWNTIME

The system downtime and nonavailability can be categorized under two different topics—scheduled and unscheduled.

Scheduled Downtime

Scheduled downtime and nonavailability include the time for system saves, scheduled maintenance for the equipment, and scheduled processing preparation. You will include scheduled downtime on the monthly production schedule when the requirement is known in time. You may also add it to a workload schedule when needed.

Unscheduled Downtime

Unscheduled downtime and nonavailability include the system being down because of power failures, the loss of air conditioning, or rebooting the system. They may also include system degradation because apiece of equipment is down, even though the system can still be used for production. Since unscheduled downtime is not something you can plan for, you will have to react, replan schedules, and advise users of changes when their work and/or deadlines will be adversely affected. If you are using an automated system, it is usually a simple task to produce a new schedule. You can usually direct the system with a command or two to produce a new schedule or a simulated schedule. In a manual scheduling system, it will require some cooperation between the subsystem coordinators and AIS operations to replan the schedule to get all the work done in a timely manner.

HELP-DESK SUPPORT

The help-desk procedures we talk about here are those relating primarily to online users. To help your operators communicate effectively with online users, you will want to have procedures established for them to follow. To develop help-desk procedures, keep several steps in mind. These steps include logging the problem, researching the problem, fixing the problem, and analyzing the problem for possible changes to training and/or documentation. Once the problem has been fixed, the operator will notify the user that processing may be continued. You will want to monitor the help-desk support for its effectiveness and to provide feedback to, and receive feedback from, the users, subsystem coordinators, and managers as well as your own staff.

Logging the Problem

The operator logs a problem to document its occurrence and to provide the information needed to solve the problem. The information includes the abort code, what step in processing the user was doing, what system the user was on, and what corrective action was taken. Figure 1-7 is an example of a log sheet that can be used for making entries. This log provides a tracking system for user problems and can be used to show if a pattern is developing. If a pattern develops, this log will provide the necessary background information needed when the programmer is notified.

DATE	USER	TERMINAL #	ABORT CODE	SYSTEM	CORRECTIVE ACTION TAKEN

Figure 1-7.—Help-desk log.

Researching the Problem

In researching the problem, you will need the abort code. With the abort code, you can determine the cause and what action will need to be taken to get the user processing again.

Solving the Problem

To solve the problem, the operator may have to reboot the computer, reload a disk file, contact the programmer, or have the users restart processing. All these solutions are dependent on what the abort code is.

Monitoring Help-Desk Support

You will need to review the help-desk log to determine if the problems reported can be corrected by changing or adding a training program. To solve the problem, you may need to update the program documentation to show the problem and its cause and solution. Be sure the users are receiving the types and levels of support they need. Listen to them. Ask if they are satisfied with the help-desk support. What else do they need? Listen to your staff, get their ideas, and work with them to continually improve support.

PRODUCTION CONTROL

When you hear the term *production control*, you usually think of the quality of the facility's output products. This is not the only area of concern. You should be looking at all areas of production, particularly daily operations.

DAILY OPERATIONS

You will want to look at the previous day's log. Evaluate what happened.

- Were all scheduled jobs run?
- When something went wrong, was the user notified?
- What action was taken to correct the problem?
- Was the job rerun?
- Was it necessary to rerun a series of jobs? If so, was it done?
- Are there corrections/adjustments you need to make to the workload schedule for today?

Remember, you are responsible for overseeing the work accomplished. Provide feedback to the production control coordinator, I/O control clerk, and shift supervisor, as needed, to improve performance and operation.

- Talk to the subsystem coordinators; are they satisfied with the service and the products?
- Look carefully at new applications:
  - How does the new application affect the other applications running concurrently?
  - Can the system efficiently handle the new work or do adjustments need to be made to the job mix and schedules?
  - What is the impact of the new application on online user response time?
- Look carefully at modified applications:
  - What is their impact on the system?
  - Does it take more or less time to process the modified applications?
  - Were any problems encountered?
  - Do you need to talk to users about the impact of changes on the overall workload or throughput time?
- Look for trends in the production process:
  - Are there times when the system seems overloaded and slow?
  - Are jobs backlogged that must be run the next day?
  - Are there times when the system is almost idle?

Your review of daily operations and asking yourself these questions will provide valuable input to that process as well as having an impact on how jobs will be scheduled in the future.

OUTPUT REPORTS

Output reports can be broken into two major categories—management and customer/user reports.

Management Reports

Management reports are usually a consolidation of information prepared for presentations and briefings. These reports sometimes require a cover letter or your comments as to the content. You will need to review

the data contained in the reports to make sure it is valid. You will also be responsible for ensuring that the reports are complete and presentable. When we say presentable, we mean readable—all the characters are there and can be read. It would be unprofessional to submit these reports in less than perfect condition.

Customer/User Reports

Being involved in a customer-oriented service, you have overall responsibility for ensuring the quality of all the products prepared in the AIS facility. The main complaints from users are poor print quality, missing pages, and poor alignment of the printing. Remember, this checking applies to all reports that leave the AIS facility. Be sure your operators, production coordinators, and I/O control clerks know the standards of quality expected. Ensure they are checking the products during processing and before sending them to the customer/users.

AUTOMATED INFORMATION SYSTEM (AIS) REPORTS

You will be expected to prepare a variety of reports. It will be your responsibility as a technical AIS manager to report to upper management on the status, performance, equipment inventory, and requirements of the AIS facility. At a minimum, you should include information concerning your areas of responsibility including user-related information. The form of these reports is the responsibility of each parent command's upper management. We can only provide examples and general suggestions, not authoritative guidance.

Reports should be regular, concise, and graphical, if possible. The amount of information you report should not exceed upper-management's requirements. "Too much, too often" is a problem common to many performance reporting schemes. Information should be easy to understand, but sufficient to support the decision-making process. The reports should compare the facility's current level of performance against a set of predefined performance goals.

Examples of reports needed for management of an AIS facility include the following:

- Hardware and software projection reports;
- Application software performance reports;
- System utilization reports; and
- Operating system software reports.

HARDWARE AND SOFTWARE PROJECTION REPORTS

Along with life-cycle management, you will be required to prepare reports to project what hardware and software will be needed to meet the command's future missions. It is important to keep this in mind as you submit the Abbreviated System Decision Paper (ASDP), as required by *Life Cycle Management Policy and Approval Requirements for Information System Projects,* SECNAVINST 5231.1. The following is a brief overview of a portion of what is required in the ASDP:

1. Outline the need for automation as it relates to specific elements of the command's mission. Summarize the fictional requirements and information-dependent tasks.
2. Summarize the selected Federal Information Processing (FIP) resource solution (functional requirements of the hardware and software) intended to satisfy the information processing need. Explain the acquisition strategy, indicating whether acquisitions will be competitive or noncompetitive and from what source the hardware and software may be acquired.
3. Summarize the projected costs (personnel, hardware, software, security mechanisms, and facilities) associated with developing an operational system.
4. Include any additional information that will facilitate understanding and evaluating the information system proposal. Training, security, privacy, maintenance, mobility, and site preparation should be addressed.

You will be expected to have the insight to predict the future, since the users will not always know what they will need later.

APPLICATION SOFTWARE PERFORMANCE REPORTS

Management will require reports that show whether the application software in use is performing as designed. Here are two items of information to include in these reports:

- Average length of time any particular job remains in the system; and

- How long a priority job (priority 1, 2, and 3) waits to be run.

This information can be used to change your existing standard operating procedures (SOPs) and aid in preparing schedules. For example, you might want to change the maximum time a priority job waits to be run.

HARDWARE UTILIZATION REPORTS

In addition to the application software performance reports, you will prepare the reports that cover hardware utilization. Your hardware utilization reports should include the following types of information:

- The amount of system idle time;
- The amount of system setup time;
- The amount of system production time;
- The amount of downtime, not only for the whole system but also for each particular piece of equipment. (This could help you explain why the idle time seems unusually high, if it does.)

This information can help you schedule the work for your system. Keep in mind that under-utilization of hardware can result in a loss of equipment and/or personnel. Equipment may be removed if it is not being fully used. If you aren't doing the amount of work for the number of people assigned, you may have billets taken away.

OPERATING SYSTEM SOFTWARE REPORTS

Operating system software reports are primarily used for the AIS facility's research. They can cover such problems as hardware under-utilization and application software aborts.

Hardware under-utilization can be measured by excessive idle time. This can be caused by no jobs to be run or no users logged on. Also, constant or excessive downtime for a specific piece of equipment with no effect on production will be considered as a waste of hardware.

Some of the most common problems that result in application software aborts are as follows:

- **Wrong file specified.** The wrong-file-specified abort can be caused by transposing the characters in the file name or inputting an old file instead of the new file.
- **Job run out of sequence.** The job-run-out-of-sequence abort can be caused by the schedule being incomplete, not listing all the jobs, or the schedule not being turned in on time. Another cause might be an inexperienced operator running the wrong job.
- **File currupted.** The file-corrupted abort is normally caused by a system failure. This can be the result of a disk head crash, the loss of power, or a power fluctuation.
- **File not available.** The file-not-available abort is caused when the input file was not received or when the job was run out of sequence and the input file has not been created yet.
- **Out of free disk space.** The out-of-freeidisk-space abort is usually a result of poor housekeeping techniques. For example, files that are no longer needed have not been removed. Be sure housekeeping tasks are performed on a regular basis. This problem also can be remedied by using some of the performance-tuning initiatives discussed later in this chapter.

These operating system software reports are a good source of information for preparing the management reports and aiding in the performance-tuning initiatives. We also need these reports for background information for submitting trouble reports, which are covered later in this chapter.

EQUIPMENT INVENTORIES

With the ever-increasing need to trim the budget, AIS resources have become a critical area. This is causing a real need for accurate and complete computer hardware inventories. We must verify the accuracy of these inventories annually to ensure we can support our command's mission.

When new equipment is acquired, it is to be added to the inventory. The inventory will contain such information as:

- Manufacturer;
- Type of equipment;
- Model number;
- Serial number;
- Minor property number;

- Location; and
- custodian.

Normally, a complete inventory is conducted annually, with spot inventories conducted periodically throughout the year. All of this will be controlled by your local SOP.

PERFORMANCE-TUNING INITIATIVES

The reports we have covered are good sources for determining what performance-tuning techniques to implement. Now let's look at some performance-tuning choices available, both hardware and software. Be sure they are authorized by your command before implementing them.

HARDWARE

Three possible hardware choices are as follows:

- Increase computer memory;
- Reduce file fragmentation; and
- Add or change a disk drive.

Increase Computer Memory

To increase a computer system's memory, we can add memory chips or memory boards. This will allow us to run larger, more complex programs on the system. We can also create cache memory, which is used with the central processor to improve execution speed and enhance central processor performance. This is accomplished by reducing the access time required to repeatedly fetch frequently used information stored in main memory. For average program mixes, cache memory yields a 50-percent increase in processing speeds. The cache memory is a random-access memory (RAM) buffer that provides high-speed storage capabilities from main memory and makes this data available to the central processor with a private central processor/cache interface.

Reduce File Fragmentation

File fragmentation occurs when you delete a file, leaving, basically, a hole in the information on the hard disk, or when you add information to an existing file when there is no contiguous space left next to the file. To correct fragmentation, you can make a backup, reformat the hard disk, and restore your files. You can also run a software program referred to as a *defragmenter* to reorganize the files so the data in each file is contiguous.

Add or Change a Disk Drive

By adding a new disk drive or replacing a disk drive with a larger drive, you will reduce the problems you may have with disk space. Remember, if you add or change a disk drive, you must modify the system setup so the system will recognize the new drive.

SOFTWARE

Let's look at some operating system changes available. Remember, anytime you are preparing to make changes to your operating system, you must consult the system operator manual first. It will show you what can and cannot be changed on your particular system. The operating system changes you can make are as follows:

- Reconfigure the system;
- Change buffer sizes;
- Change memory addresses.

Reconfigure the System

When we reconfigure the system, we can move the device drivers into extended memory. We can move disk files from a smaller capacity disk drive to a larger capacity drive; this will also help with fragmentation.

Change Buffer Sizes

By changing buffer sizes, we increase the input/output activity of the system, resulting in the job finishing faster. This will also help reduce the chances that the system will lock up.

Change Memory Addresses

By changing memory addresses, you can tailor extended and expanded memory to the system's needs. This results in freeing memory for the execution of production jobs.

TROUBLE REPORTS AND TECHNICAL ASSISTS

You will be responsible for submitting trouble reports on software and hardware problems. Remember to follow the instruction from the command receiving the trouble report. In most cases, this will be the Navy Maintenance and Supply Systems Office (NAVMASSO). As shown in figure 1-8, the trouble report contains a lot of information. Items 13, 14, and

TROUBLE REPORT/CHANGE PROPOSAL

1. CONTROL NO.: _____ 2. ( ) TR ( ) CP

3. PRIORITY: ( ) CRITICAL ( ) URGENT ( ) ROUTINE

4. REPORTING ACTIVITY: _____ 5. UIC: _____ 5a. TYCOM: _____

6. POINT OF CONTACT: _____ 7. TELEPHONE NO.: _____

8. LOCATION: _____

9. REPORTING METHOD: ( ) PHONCON ( ) LETTER ( ) MESSAGE ( ) VISIT

10. PROBLEM TYPE: ( ) HARDWARE ( ) APPLICATION SOFTWARE ( ) SYSTEM SOFTWARE
( ) DOCUMENTATION ( ) PROCEDURES

11. PROBLEM DESCRIPTION: _____

_____

_____

_____

_____

_____

_____

12. SYSTEM CONFIGURATION DATA:

A. HW: ( ) SNAP I ( ) SNAP III

FAILED COMPONENT NAME/SERIAL NO.: _____

B. SW: SYSTEM/SUBSYSTEM: _____ RELEASE/VERSION: _____

MODULE/SEGMENT: _____ ACCESS LEVEL: _____

OPTION/SUBOPTION: _____ SCREEN/TRANS NO.: _____

C. DOC: REFERENCE: _____ DATE: _____

CHANGE NO.: _____ PAGE/PARA.: _____

SCREEN	PF KEY	SCREEN	PF KEY
1.	/	4.	/
2.	/	5.	/
3.	/	6.	/

==========

13. DATA:

( ) CORE DUMP ( ) SOURCE DOCUMENT ( ) CONSOLE LISTING
( ) PROGRAM LISTING ( ) PARAMETER CARDS ( ) SYSTEM BACKUP TAPE
( ) INPUT DATA ( ) OUTPUT DATA ( ) REPORT

14. RECEIVER'S NAME/CODE: _____ DATE/TIME REC'D: _____

15. ASSIGNED TO: NAME: _____ DTG: _____

CODE: _____ PHONE: _____ DTG: _____

Figure 1-8.—Typical trouble report form.

15 are reserved for the receiving command's use. Most of the items are self-explanatory, but let's cover two that aren't as obvious.

Item number 3 asks for the priority assigned. Critical means that you cannot work around the problem to continue operating. Urgent means that you can work around the problem, but a resolution is required immediately. Routine means the correction is needed, but you can work around the problem and live with it until it is fixed.

When you start to fill in item 11, remember to enter a complete, detailed description of the problem you are experiencing. Include the screen or menu number, if applicable, the option number, if applicable, and any error message received.

Various procedures will have to be followed for personal computers (PCs), depending on the problem. For commercial software problems, inform the software manufacturer of the problem giving as much information as possible. Normanlly, the manufacturer will tell you how to correct the problem over the phone, or if the problem will be corrected with the release of the next version of the program. For hardware, it is usually covered by either a maintenance contract or manufacturer's warranty. With a maintenance contract, you will follow the instructions for repair as outlined in the contract. The owner's manual of equipment covered by a manufacturer's warranty will have a phone number to contact a repair technician.

SOFTWARE TROUBLE REPORTS

Normally, the trouble reports for the software are submitted by that subsystem's coordinator, after notifying the AIS facility.

Some of the most common trouble reports for software include the following:

- Monthly files are not being cleared at the beginning of the new month.
- Report titles are wrong.
- Bad data was entered into a file and cannot be removed through normal procedures.

HARDWARE TROUBLE REPORTS

It is the AIS facility's responsibility to submit the trouble reports on system hardware problems. The common reasons for hardware trouble reports include the following:

- A file has become corrupted and no good save tapes are available to rebuild the file.
- The system keeps hitting 100 percent of capacity and locks up.
- The system keeps dropping I/O channels.

If the hardware problem can be traced to a specific piece of equipment, notify the maintenance technicians to handle the problem.

TECHNICAL ASSISTS

After submitting a trouble report, you will need to coordinate with the central design activity to see if the problem can be taken care of over the phone or if it will require a technical assist. If it requires a technical assist, there may be a requirement to arrange for transportation, entry to the facility, and/or escorts. You will need to schedule time for the technician to use the system and notify the users that the system is unavailable.

OPERATIONAL GUIDELINES

When preparing the operational guidelines for your facility, you should consider four major areas as follows:

- Future growth capabilities;
- Backup operations;
- Contingency plans and disaster recoveries; and
- Emergency responses.

To develop these and other operational guidelines, you will need to review the current SOPS, command's mission, run folders, and monthly production schedules. While reviewing these, you are looking to make sure that the current and/or proposed operational guidelines will allow the AIS facility to meet the command's mission.

FUTURE GROWTH CAPABILITIES

Projecting future growth capabilities is often the most overlooked operational guideline. Projecting future growth should have been done when the system was designed, but it can be done at anytime it is needed.

Users are one of your last sources of information when it comes time to start projecting. They know how their workload has increased in the past and can forecast what it will be in the future. With this information, and

by knowing the limitations of the existing system, you can project what additional equipment will be needed to handle the future workload of the command.

This may include additional network drops and terminals located throughout the command, spare parts, backup media, and personnel. The most important thing to remember when projecting the future growth capabilities is to take your time when doing the research. You don't want to come up short when requesting the additional materials that you expect to need later on.

BACKUP OPERATIONS

Backup operations fall into two categories: normal and special saves.

Normal saves. Normal saves are the ones worked into the monthly production schedules. These saves are normally done every day or night and are the most important recovery tool available to you.

Special saves. Special saves are the ones that need to be done before and after the implementation of a software upgrade and during monthly and yearly production runs. The saves that are done in association with a software upgrade are not covered on your production schedule, since upgrades are not released on any published schedule.

CONTINGENCY PLANS AND DISASTER RECOVERIES

The most important part of disaster recovery is having a contingency plan and current backup files. The AIS facility's contingency plan covers what is required to get the facility back online as soon as possible. Your contingency plan should include emergency response, backup operations, and recovery plans. To have current backups, we must ensure that normal saves are done as scheduled. The saves can be categorized as either whole system or data file saves. The AIS facility's resources, schedule, and instructions will be the governing factors as to which category of saves and the frequency with which the saves will be done. For further guidance, as to the minimum frequency and the category of saves, refer to the local type commander's (TYCOM) instructions.

Another part of the recovery process is making sure that replacement parts are available. There are constraints as to the number of parts maintained onboard your activity. Before a major deployment (or periodically for shore activities), it is important to take an inventory of the parts so if the parts are not on board, they can be ordered.

EMERGENCY RESPONSES

The last major area we are going to look at is emergency response. When a problem occurs, such as a job aborts or the system goes down, the steps you and your AIS staff must follow are:

1. **Log the problem.** A good rule is to log everything; this can save time and help to identify problems early.
2. **Notify management, users, and the maintenance technician.** By notifying management, you provide them the information they need to answer questions and make decisions concerning the system. If the users are kept informed, they won't be as apt to keep calling the operators when the operators are busy trying to get the system back up and running. In notifying the maintenance technicians, whether hardware or software, you need to tell them what you were doing, exactly what happened, and what you have tried to do to fix the problem.
3. **Adjust staffing when possible.** Adjusting staffing works in two ways. If the system is going to be down for an extended period of time, it is a waste to keep all the operators there with nothing to do. Likewise, there are times when additional expertise will have to be brought in to help get the system up and running. Either way, this will be your decision as the AIS facility manager. You will have to analyze the situation and decide what skills are needed to solve a problem, who has the skills, who is available, how many personnel are needed, and so on.

EMERGENCY URGENT CHANGE REQUESTS

Occasionally, the best-laid plans will have to be changed. One of these times is when an emergency urgent change request (priority job) comes in. Normally, there is a good reason for each emergency urgent change request. These change requests cover both application and system programs.

For application programs, some reasons for urgent change requests are a special report needed for a meeting, last-minute corrections before starting a monthly or yearly job, and a deadline that is moved to

an earlier time. Invariably, a priority job comes in that must be run just when the shift is almost over. Being a customer-oriented service, it is our job to get the product out.

With system programs, three common reasons for urgent change requests are special saves, changes to the operating system, and system testing by NAVMASSO.

SUMMARY

Scheduling is the interface between the user, I/O control, and computer operations. The scheduler's job is to follow the AIS facility's scheduling procedures to develop daily, weekly, and/or monthly production schedules.

You will be depended on to effectively and efficiently schedule the computer and other related resources of your AIS facility to meet user processing requirements.

Input/output control is an important AIS function. It is the point of contact for AIS users (customers). Like in any other business, customers must be treated with courtesy, tact, and diplomacy. It is the I/O clerk's job to receive jobs from users; maintain logs, prepare jobs to be run on the computer; make sure everything is ready on time; communicate with users on job requirements and problems; and check, prepare, and distribute output products.

Each of the I/O control clerk's tasks may involve customer liaison. Maintaining good customer relations is as important as processing the customer's jobs.

We talked about different types of reports, performance-tuning initiatives, application software libraries, trouble reports and technical assists, operational guidelines, and emergency change requests. This is, by no means, a complete list. As you continue in your career, you will be adding new skills and more responsibilities to these. This chapter gives you the foundation needed to build on, with the skills you have and those you will learn.

CHAPTER 2

COMMUNICATIONS ADMINISTRATION

LEARNING OBJECTIVES

Upon completing this chapter, you should be able to do the following:

- *Identify the background and mission of the departments within the National Communications System.*
- *Identify the mission and policy of naval communications.*
- *Identify the functions of the Naval Telecommunications System and the roles of communications management personnel.*
- *Identify the elements and responsibilities related to standard message processing.*
- *Identify the procedures for minimize consideration and processing of messages.*
- *Identify the procedures used for general administration and handling of communication files.*
- *Identify the procedures used in communications planning.*
- *Identify the procedures for conducting watch-to-watch inventories and updating the NWPs.*
- *Identify the role of the naval warfare publications library (NWPL) including NWPL administration and maintenance.*

"Naval communications" is the term assigned to the entire communications effort of the Department of the Navy, both afloat and ashore. The naval communications complex is the total of all Navy-operated communications installations and services. The communications complex provides, operates, and maintains tactical communications, including fleet broadcast, ship to shore, and air to ground. The operating forces and all commands and activities ashore depend on this complex for reliable transmission and receipt of information.

In this chapter, we will give you a broad overview of how naval communications is organized at shore commands and aboard ship. We will also discuss the various publications used in naval communications. These publications provide standard guidance for all phases of naval communications, such as basic communications doctrines, message preparation, and proper circuit discipline.

NATIONAL COMMUNICATIONS SYSTEM

The National Communications System (NCS) was established to achieve a cohesive effort in the event of war. The NCS provides a unified governmental system that links together the communications facilities and

components of the various Federal agencies. Essentially, all branches of the Federal Government, both civilian and military, are part of the NCS. Each department and branch, however, has its individual organization, methods, and procedures.

DEFENSE COMMUNICATIONS SYSTEM

The Defense Communications System (DCS) exists to support the three military departments (Navy, Army, Air Force) and other Department of Defense activities. The circuits that make up the DCS are government-owned or leased and are point-to-point circuits that are long-haul and worldwide. The DCS combines many of the communication elements of the three military forces into a single communications system.

Although the Naval Telecommunications System (NTS) and the DCS are two different communications systems (fleet and ashore, respectively), they are constantly intermixed. For example, as often happens, a naval message originated aboard ship and destined for a shore activity leaves the ship over the NTS, but final routing is accomplished over the DCS circuits. The interface between the NTS and DCS is always provided by the shore communications facility.

DEFENSE INFORMATION SYSTEMS AGENCY

The Defense Information Systems Agency (DISA) gives operational direction to the DCS. With reference to the DCS, the DISA must ensure that the system is operated and improved so as to meet the continual long-haul, point-to-point requirements that arise.

The DISA functions under the management of a director who is appointed by the Secretary of Defense. The director is a flag-rank officer and is responsible for coordinating the combined communications elements of the three military departments.

MISSION OF NAVAL COMMUNICATIONS

The mission of naval communications is to provide and maintain reliable, secure, and rapid communications, based on war requirements, to meet the needs of naval operating forces. Naval communications must also satisfy the requirements of the Defense Communications System (DCS) and the National Communications System (NCS).

Naval communications must always be ready to shift to the requirements of wartime. Our peacetime organization and training must be capable of making this shift rapidly and with a minimum of changes. Without this capability, our forces would be severely handicapped, and vital defense information would never reach its destination. For this reason, we have a well-defined communications structure, with responsibilities assigned to each element, from the Chief of Naval Operations (CNO) down to individual fleet units.

POLICY OF NAVAL COMMUNICATIONS

The policy of naval communications is to:

- Establish and maintain effective communications within the Department of the Navy;
- Encourage at all levels of command an effort to improve techniques, procedures, and efficiency;
- Cooperate with the military services, Defense Information Systems Agency (DISA), and other departments and agencies of the U.S. Government and allied nations;
- Encourage development of the amateur and commercial communications activities of the United States to enhance their military value and to safeguard the interests of the nation; and
- Promote the safety of life at sea and in the air by maintaining communications facilities with the U.S. Merchant Marine, aircraft over sea, and appropriate U.S. and foreign communication stations.

NAVAL TELECOMMUNICATIONS SYSTEM

The word “telecommunications” includes all types of information systems in which electric or electromagnetic signals are used to transmit information between or among points. The Naval Telecommunications System (NTS) is comprised of all the end terminal processing equipment, transmission, switching, cryptographic, and control devices used to transmit operational information in the Navy.

The NTS provides electrical and optical communications from the commander in chief and naval commanders down to all naval forces under its command. You should remember that the NTS is used primarily to exercise command and control over the naval operating forces; not the shore establishment. Most shore establishments are served through the Defense Communications System (DCS). Naturally, there are overlapping portions of each system where necessary.

Operational direction and management control of the assigned elements of the NTS are the responsibility of the Commander, Naval Computer and Telecommunications Command (COMNAVCOMTELCOM).

In naval communications, COMNAVCOMTELCOM determines the responsibilities of each of the various commanders, whether a fleet commander or the commanding officer of a ship. For example, direction and control of all naval fleet broadcasts, ship shore, air-ground, and other direct fleet-support telecommunications are assigned to the fleet commanders in chief. That is to say, all Pacific Fleet naval broadcasts are under the operational direction and control of the Commander in Chief, Pacific Fleet (CINCPACFLT). The same applies to Atlantic Fleet navak broadcasts. These broadcasts are under the operational direction and control of the Commander in Chief, Atlantic Fleet (CINCLANTFLT).

Fleet commanders in chief are responsible for the adequacy of communications to satisfy the needs of their respective fleets. They, in turn, assign broad communications responsibilities in the form of fleet operation orders (OPORDs). OPORDs are to be complied with at every level down through individual commanding officers of operating ships.

The commanding officers use only those portions of the fleet commander's communications OPORD that affect them. In this simple, yet direct, manner, the NTS is administered at every operational level in the fleet, according to that ship's mission and communication needs. We will talk more about OPORDs later in this chapter.

The Naval Telecommunications Command is composed of the following elements:

- Commander, Naval Computer and Telecommunications Command (COMNAVCOMTELCOM);
- Naval Computer and Telecommunications Area Master Stations (NCTAMSs);
- Naval Computer and Telecommunications Stations (NAVCOMTELSTAs, sometimes referred to as NCTSs);
- Naval Communications Detachments (NAVCOMTEL DETs, also abbreviated NCTDs);
- Naval Data Automation Commands (NAVDACs);
- Naval Security Group Departments (NAVSECGRUDEPTs) of NAVCOMTELSTAs; and
- Navy-Marine Corps Military Affiliate Radio System (MARS).

COMMANDER, NAVAL COMPUTER AND TELECOMMUNICATIONS COMMAND

With the merging of Automated Information Systems (AIS) and telecommunications, the mission and responsibilities of COMNAVCONTELCOM have greatly increased. You will see COMNAVCOMTELCOM continue to change and grow as telecommunications technology advances into the 21st century.

There have already been changes in the makeup of the COMNAVCOMTELCOM claimancy as communications stations have merged with Naval Regional Data Automated Centers (NARDACs). Those communications stations that do not merge with an AIS activity will become Naval Computer and Telecommunications Stations (NCTSs) or Naval Computer and Telecommunications Detachments (NCTDs).

Although not all-inclusive, COMNAVCOMTELCOM's responsibilities include the following:

- Integrates and consolidates Navy common-user ashore communications and information resources (IR) (including personnel) into the NAVCOMTELCOM claimancy, and implements Navy IR management policy within the claimancy;

- Advises the Director, Naval Space and Warfare Command, of validated communications requirements that may demand development or modification of satellite communications systems;
- Formulates policy on, and exercises authoritative control over, the Navy Communications Security Material System (CMS), and reviews or initiates action in cases of loss or compromise of CMS material;
- Serves as Department of the Navy (DON) manager of leased portions of Navy dedicated and common-user information transmission systems;
- Manages the Navy and Marine Corps Military Affiliate Radio System (MARS) and coordinates Navy participation in amateur radio matters;
- Establishes, implements, and maintains the Fleet Operational Telecommunications Program;
- Manages International Maritime Satellite (INMARSAT) communications ground interfaces to naval communications for the DON and handles any other commercial telecommunications authorized by law or treaty;
- Operates and maintains the NCTSs, NARDACs, and assigned elements of the Defense Communications System (DCS);
- Serves as technical advisor to CNO for communications/enlisted ratings (RM, ET, and assists in career development and training for these ratings; and
- Serves as central design agency for communications in the DON, performs life-cycle management on Navy Standard Communications Software components.

NAVAL COMPUTER AND TELECOMMUNICATIONS AREA MASTER STATIONS (NCTAMSs)

As we mentioned earlier, there have been changes in the claimancy of NAVCOMTELCOM. As a result, each of the former NAVCAMS has been redesignated as a NCTAMS, and has merged with a NARDAC. The four NCTAMSs are NCTAMS EASTPAC, Honolulu, Hawaii; NCTAMS LANT, Norfolk, Virginia; NCTAMS WESTPAC, Guam; and NCTAMS MED, Naples, Italy.

The world is divided into four Naval Communications Areas (NAVCOMMAREAs): Western Pacific (WESTPAC), Eastern Pacific (EASTPAC), Atlantic (LANT), and Mediterranean (MED) (figure 2-l). All communications activities within any of these geographical areas are organized to operate under the operational control of a NCTAMS. These master stations are the major sites in a COMMAREA and are the primary keying stations for that area. They are the entry points for Navy Tactical Satellite Systems and also operate and maintain one or more Defense Satellite Communications System (DSCS) terminals.

The NCTAMSs have, as part of their organization, a fleet telecommunications operations center (FTOC). This is the focal Point for fleet communications support.

To support the operating forces of each fleet commander in chief (FLTCINC), the authority to exercise operational direction over all NAVTELCOMs is delegated on an area basis to the commanding offiers of the master stations. Operational direction is decentralized down to the commanding officers of the NCTAMSs. These commanding officers report to and are immediately responsible to the FLTCINC. COMNAVCOMTELCOM, however, exercises overall operational direction to assure integration of the worldwide system, taking into consideration the requirements and priorities of other FLTCINCs and/or higher authority. You should refer to the appropriate Fleet Operational Telecommunications Program (FOTP) manual for futher information.

Within the various NAVCOMMAREAs are alternate NCTAMSs. They coordinate control of communications under the direction of the primary NCTAMSs.

NAVAL COMPUTER AND TELECOMMUNICATIONS STATION

A Naval Computer and telecommunications Station (NAVCOMTELSTA) is a communications station with the primary responsibility for communications in a large specific area. This responsibility includes all communications facilities and equipment required to provide essential fleet support and fixed communications services. For example, NAVCOMTELSTA, Diego Garcia, serves a large geographical area of the Pacific and Indian oceans. It also includes facilities and equipments necessary to interface with all other NAVCOMTELSTAs or

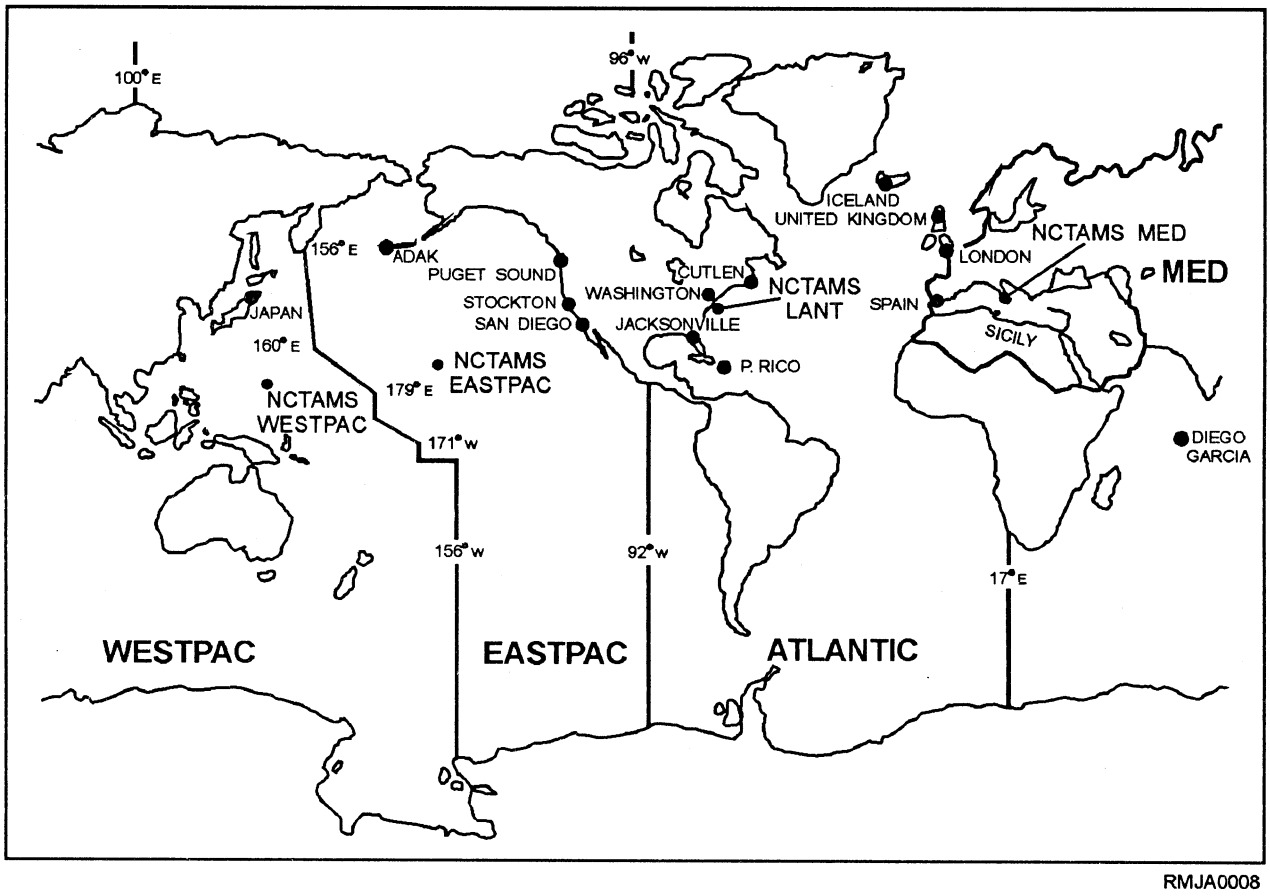


Figure 2-1.—Naval communications areas.

communications detachments on all naval communications matters. It also provides Naval Industrial Fund (NIF) AIS services to Navy customers.

NAVAL COMPUTER AND TELECOMMUNICATIONS DETACHMENT

A Naval Computer and Telecommunications Detachment (NAVCOMTELDET) is a small telecommunications facility that is assigned a limited, or specialized, mission and has a limited number of personnel and facilities.

NAVAL DATA AUTOMATION FACILITY

A Naval Data Automation Facility (NAVDAF) comes under the control of an NCTS or a NARDAC. NAVDAFs provide AIS services in areas where no NARDACs are located. The workload of a NAVDAF is normally less than that of a NARDAC.

NAVAL SECURITY GROUP DEPARTMENTS

The Naval Security Group Departments (NAVSECGRUDEPTs) come under the authority of Commander, Naval Security Group Command (COMNAVSECGRU), and are responsible for the cryptologic and related functions of the Navy. NAVSECGRUDEPTs maybe part of a NCTAMS or a NAVCOMTELSTA. As such, COMNAVSECGRU exercises technical control over the cryptologic operations, whereas COMNAVCOMTELCOM has overall responsibility for the management and operating efficiency of the NAVSECGRUDEPTS.

MILITARY AFFILIATE RADIO SYSTEM (MARS)

A function of the Military Affiliate Radio System (MARS) is to provide auxiliary communications to military, civil, and/or disaster officials during periods of emergency. The Navy encourages amateur radio operators to affiliate with MARS. Many of the

operators have earned their amateur radio licenses from the Federal Communications Commission.

The amateur radio operators, using their amateur stations on Navy radio frequencies, receive training in naval communications procedures and practices. Besides assisting in emergency situations, MARS operators also create interest and furnish a means of training members in naval communications. You can find detailed information about the MARS program in *U.S. Navy-Marine Corps Military Affiliate Radio System (MARS) Communications Instructions,* NTP 8.

NAVAL COMMUNICATIONS MANAGEMENT

As radiomen advance, they can expect to assume additional authority and responsibility. A first class or chief will most likely be placed in charge as a watch supervisor, leading petty officer or chief, or even as a division officer. These are only a few of the many leadership positions to which they might be assigned. In summary, eventually, a career Radioman is going to be a manager.

The Navy has conducted extensive studies to pinpoint problems in the area of communications organization and management. These were done to allow communications personnel to take corrective action on the problem areas. Use of sound managerial principles helps us accomplish our mission.

All levels of management require an evaluation standard. Managers are then able to properly evaluate specific communication systems or components. Such an evaluation provides a basis for comparison of equipment, personnel, and even complete facilities. This evaluation forms the basis for establishing additional standards and guidelines. A continuing evaluation requires data collection via a system of feedback reports from all managerial levels.

EVALUATING PERFORMANCE

Effectiveness of naval communications is the first consideration in the management of any communications facility. The overall capability must be viewed in relation to each functional unit. Standards of performance can be established and control elements determined. An evaluation of the entire system must be completed by the highest level of command. Each operational unit must be scrutinized by the chief or first class in charge.

Establishing Standards

Standards of performance must be established to determine the effectiveness of operations and service provided against customer requirements and system capability. Standards must be established for internal functions as well as for overall system performance. After performance standards are established, the control elements and manner of control can be determined.

It is most important that performance standards be established in the general areas of reliability, speed, security and economy. These areas can be broken down into standards for internal operation, equipment, personnel, maintenance, supply, and so forth.

Realistic standards of performance must be established. This allows maximum use of resources without overcommitment. The standards must be compatible with command requirements and within resource capability. The standards must also be flexible enough to allow for changing operating conditions. Skill levels and manning levels change constantly. Equipment status and configurations are never stable. Operating conditions and commitments change from day to day. Therefore, each communications facility manager must establish flexible standards to accommodate changing requirements and situations.

Management Responsibilities

Mid-management radiomen must realize the need for progressively improving standards. The following points may assist mid-management radiomen in improving standards within their division:

- **Overcoming Resistance—** The practice of relying on past performance as a basis for establishing standards is often sound. With an organized effort, however, conditions can be changed to improve performance. If the personnel responsible for better performances participate in the organized effort, the problem of resistance to higher standards is often eliminated.

- **Improving Conditions—** Owing to the rapid growth and change in the character of communications systems, considerable managerial effort must be devoted to improving the effectiveness of operations and service. The essential approach to this type of problem can be summarized in a sequence of three stages:

  — Discovery of the problems; that is, what part of an existing condition needs improving;

— Diagnosis to determine what changes are needed to bring about the needed improvement; and

— Remedial action; that is, implementing the necessary changes.

- **Responsibility—** Responsibilities must be established in accordance with the organizational structure and be clearly defined.

- **Organizational Considerations—** Leading radiomen must realize that the existing organizational structure may be a contributing factor to poor personnel performance. In such instances, recommendations to realign the organizational structure must be seriously considered.

- **Conservation of Personnel Resources—** The communications facilities manager must be constantly aware of the need to conserve personnel resources at all levels. Conservation of personnel resources is accomplished by evaluating personnel requirements properly and by using available personnel effectively through proper training and assignment.

GENERAL ADMINISTRATION

A communications facility should function effectively and efficiently. This is normally the result of the senior supervisor's ability to set up and manage the organization.

Good supervisors retain open minds. They recognize the need for change and implement those changes as required. They acquire a thorough knowledge of the functions performed by their area of responsibility and understand how it relates to the overall mission. Only then can they plan a rational approach to correct a problem or make positive changes.

Although the current structure and methods may meet the objectives of the division, a periodic review should still be conducted. The goal is to develop more efficient office methods, techniques, and routines. Procurement of state-of-the-art equipment may require a complete evaluation and reorganization of divisional workflow and workspace layout. To plan properly, the supervisor must know the following information:

- **WHAT** work is to be done;

- **WHY** the work is to be performed;

- **WHEN** the work is to be performed;

- **HOW** the work is to be accomplished;

- **WHERE** the work is to be performed; and

- **WHO** is responsible for completing the work.

PERSONNEL MANAGEMENT

Good managerial traits and supervisory abilities are prerequisites for the first class or chief petty officer who is required to function as a front line supervisor and manager. The RM1 or RMC will normally be the RM supervisor and will have many managerial and supervisory responsibilities added to those present at the junior petty officer level.

Supervision involves working with people, and a major responsibility of a supervisor is production. A good supervisor knows how to get a job done by getting the most out of personnel. However, the desire to attain an acceptable production level must not be at the expense of personnel assets. People have the right to be treated as individuals and respected as such. If treated in any other reamer, no amount of pressure will create a permanent increase in production levels. While you want to achieve a high level of production, you also want your personnel to produce willingly and be interested in their work.

OFFICE MANAGEMENT

The physical location of a communications office is normally predetermined by higher authority. Furthermore, the space allotted to the various sections is usually determined by competent engineers based on available space. After discussing the matter with the senior petty officers in the division, the division officer or division chief usually determines the physical location of furniture and equipment.

When the office layout is being planned, primary consideration must be given to proper flow of paper and work, the physical location of workspaces, and the internal communications of the division.

Secondary factors to be considered are the number of personnel to be accommodated, safety standards, security of classified material, structural location of electrical outlets, and physical locations of bulkheads and passageways.

Paper and Work Flow

Good paper flow is the smooth movement of paperwork from one desk or individual to another. As much as possible, the paperwork should flow in one direction through various sections with no reversals or

criss-crossing. Figure 2-2 shows the ideal communications space layout with sequential workflow. Placing related tasks in adjacent spaces reduces distance and increases efficiency of operations. This ultimately increases the work accomplished.

Workflow affects the placement of sections within the division and the location of desks, files, and other equipment. Changes should only be made to improve workflow. Deviations from approved methods can result in loss of time and motion and cause delays in completion of work assignments.

Physical Factors

The physical layout of workspaces should be reviewed when:

- There is evidence of improper workflow;
- The number of personnel or office procedures change;
- The volume of work increases or decreases;

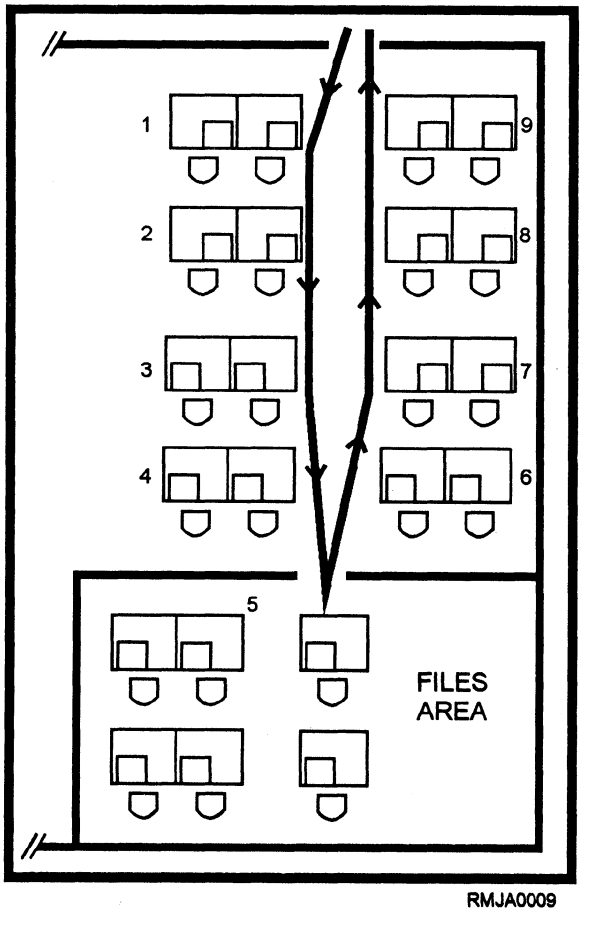


Figure 2-2.—Ideal communications space layout.

- New equipment is ordered or is to be installed; or
- There is a change in allotted space.

Before actually moving personnel or equipment, it is a good idea to draw a scale model of the anticipated layout. You can then evaluate the idea and judge its effectiveness.

In evaluating an office layout, you should consider the following factors:

- Office congestion;
- Personnel supervision;
- Use of space;
- Volume of work versus people; and
- Office appearance.

Internal Communications

A large portion of communications office work consists of receiving, distributing, and filing communications, reports, instructions, and records. Another major portion of the work is the disposition of correspondence. When handling correspondence, the supervisor must establish standard procedures. Once decided, these procedures should be conveyed both vertically and horizontally. Vertical communications are routed up and down the chain of command. Horizontal communications are routed to other divisions and departments.

Vertical communications can be either formal or informal. Formal information usually consists of office procedures, watches, schedules, job instructions, and written orders. Formal communications are handled to ensure wide dissemination and accuracy of information, to avoid distortions, and to provide a permanent record. Informal information is usually passed orally and provides guidance and instructions on work assignments.

Horizontal communications can be either formal or informal. Personnel holding parallel positions (two watch supervisors for instance) can sometimes resolve problems through informal communications without involving higher authority. On the other hand, formal communications must be used when the subject requires approval through the chain of command. Formal communications may be in the form of station directives, administrative procedures, or station watch bills.

COMMAND COMMUNICATIONS ORGANIZATION

The structure of the communications organization of a command depends on command size and whether the command is ship- or shore-based. Not all Navy ships have a communications department. *Basic Operational Communications Doctrine (U),* NWP 4 (NWP 6-01), designates the types of ship that should have a communications department. In ships that are not so designated, communications personnel are assigned to the operations department, but the communications functions are the same as those for ships with a communications department. Future organization may structure communication and automated systems into a combined information systems department.

Senior enlisted personnel may be assigned communications duties normally assigned to officers if there are insufficient officers to fill communications billets. Figure 2-3 shows a normal shipboard communications organization. Key billets are further discussed in this chapter.

Commanding Officer

The commanding officer of a ship or a shore command is responsible for the communications of that command. The only exception to this is when a flag officer is embarked aboard a ship, making that vessel the flagship. In such cases, the embarked commander assumes control of flagship communications. The commanding officer is still responsible for the proper handling of message traffic within the ship.

Communications Officer

The communications officer (COMM officer) is responsible for the organization, supervision, and coordination of the command's exterior communications. At shore stations, the COMM officer is the department head. Aboard ship, the COMM officer may be assigned as a department head or may be assigned under the operations officer. Aboard ship, the COMM officer is also responsible for the management of related internal communications systems.

Radio Officer

The radio officer is in charge of the communications center. This officer is responsible for organizing and supervising assigned personnel to ensure accurate, secure, and rapid communications. The radio officer is responsible to the communications officer for:

- Preparing the command's communications plan;

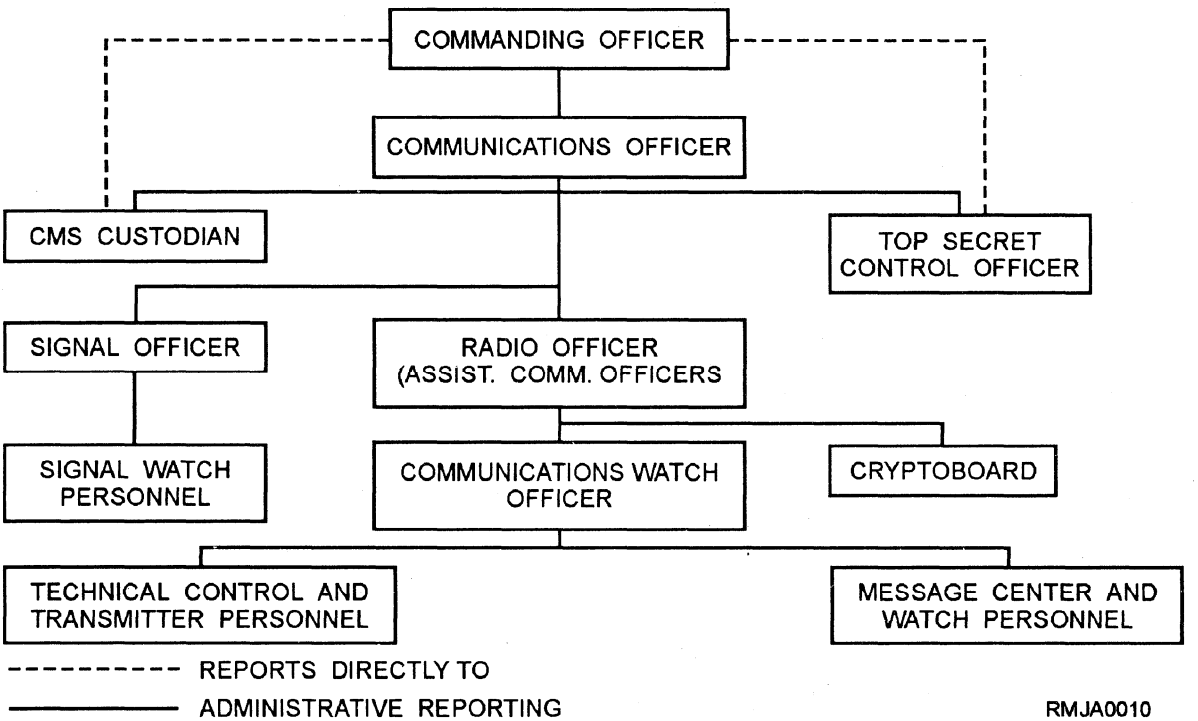


Figure 2-3.—Communications organization.

- Monitoring the proper allocation of equipment for operations;
- Preparing and maintaining the communications watch, quarter, and station bill;
- Conducting the communications training program; and
- Preparing standard operating procedures (SOPs) for the communications center.

On small ships, the communications officer and the radio officer maybe the same person.

Communications Security Material System (CMS) Custodian

The CMS custodian is responsible to the commanding officer for:

- Managing the CMS account in accordance with the instructions contained in the *Communications Security Material System (CMS) Policy and Procedures Manual,* CMS 1;
- Advising the commanding officer on matters concerning the physical security and handling of CMS publications and materials;
- Stowage of CMS publications and materials, as well as the drawing, correcting, and authorized destruction; and
- Submitting all reports concerning the accountability and issuance of CMS publications and materials.

Watch Section Personnel

The functions of the operational organization of a communications command consist of:

- Message processing, circuit operation, technical control, data processing, and operation; and
- Control of voice circuits and the operation of satellite circuits, where installed.

The combined efforts of the operational organization are performed in various spaces simultaneously. In the next section, we will discuss the duties and responsibilities of some of the key billets within this organization.

COMMUNICATIONS WATCH OFFICER (CWO).— The CWO is responsible to the communications officer for:

- Ensuring that communications capabilities are accomplished in accordance with the command's mission;
- Incoming and outgoing traffic, ensuring that all messages, transmitted or received, are handled rapidly and accurately in accordance with existing regulations; and
- Ensuring compliance with existing communications directives and monitoring the performance of on-watch personnel and spaces.

Fleet Communications (U), NTP 4, contains a detailed listing of the duties of the CWO.

SENIOR WATCH SUPERVISOR (SWS).— When assigned, the SWS is the senior enlisted person on watch in communications spaces and is responsible to the CWO for:

- The proper handling of all communications;
- Notifying the CWO on all matters of an urgent or unusual nature;
- Examining operational logs and monitoring equipment alignment and operation; and
- Directing action necessary to prevent or overcome message backlogs.

In addition to the duties listed in NTP 4, the SWS is also responsible for any other duties as maybe assigned by the CWO.

COMMUNICATIONS CENTER SUPERVISOR.— The communications center supervisor is responsible to the CWO and SWS for:

- Supervising message processing and circuit operations;
- Directly supervising all radiomen on watch in the message processing center; and
- Notifying the CWO and SWS on all matters of an unusual or urgent nature.

TECHNICAL CONTROL SUPERVISOR.— The technical control ("tech control") supervisor is responsible to the CWO for:

- Establishing and maintaining required circuits, and initiating action to restore or bypass failed equipment;

- Ensuring that quality monitoring and control procedures are used on all systems;
- Maintaining the status board showing pertinent information on all equipment, nets, and circuits in use; and
- Directly supervising all personnel assigned to technical control and transmitter room spaces.

Command Ship Communications

The term "flagship" is sometimes used instead of "command ship" but means the same thing. Either term means that a group, squadron, or division commander is embarked on board, thereby making that vessel the flagship, or command ship. We mentioned earlier that, in flagships, the embarked commander assumes responsibility for communications functions. The flag communications officer is responsible for ship and flag communications requirements. However, the internal routing of message traffic remains the responsibility of the commanding officer of the ship in which the flag is embarked.

When a flag officer is embarked, the ship's communications officer, communications watch officers, and enlisted communications personnel may be ordered to additional duty in the flag communications division. These personnel are directly responsible to the flag communications officer for the operation of the flag communications functions. The ship's communications officer reports to the flag communications officer and is the contact officer for matters pertaining to the handling of ship and staff message traffic. Figure 2-4 illustrates a standard watch organization aboard a ship with a flag embarked.

By now, you should have a basic idea of how naval communications is organized at shore commands and aboard ship. Remember that there are variations in all organizations. The command size, scope of operations, and personnel assets are just a few of the factors that affect the structure of the communications organization.

OPERATION ORDERS

Operation orders (OPORDs) are directives issued by naval commanders to subordinates for the purpose of effecting coordinated execution of an operation.

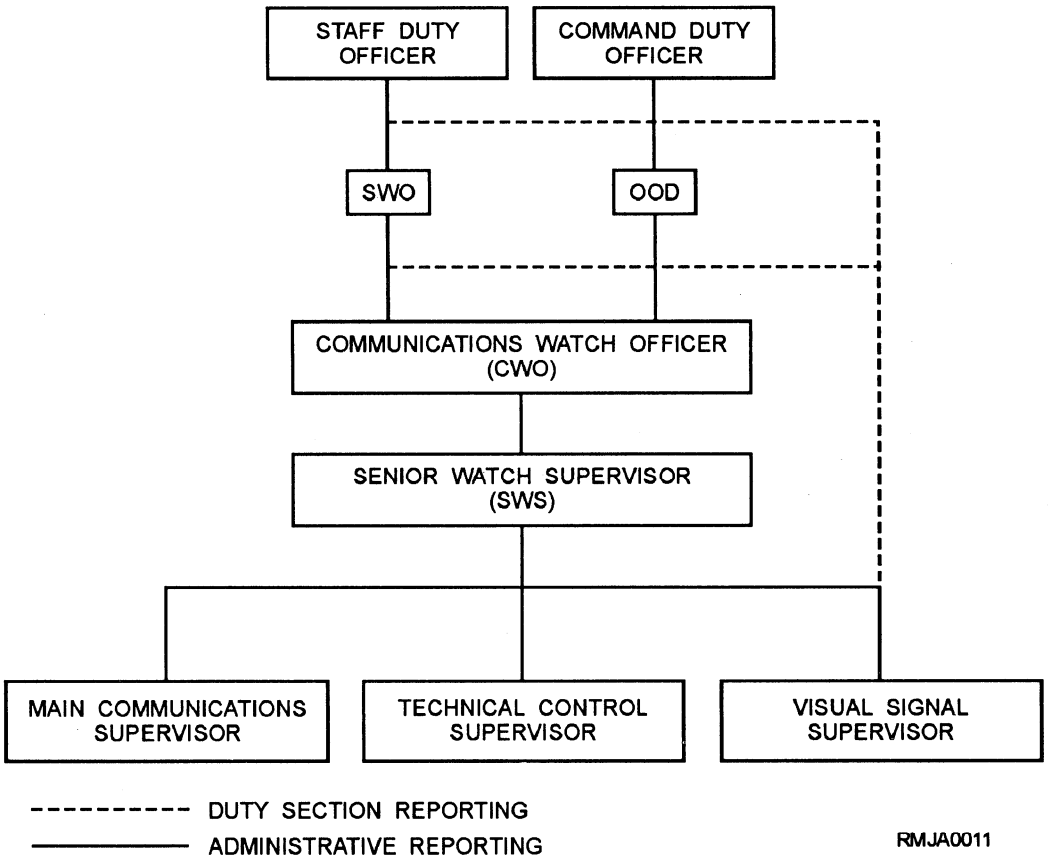


Figure 2-4.—Communications watch organization.

Operation orders are prepared in accordance with a standing format, as set forth in *Naval Operational Planning,* NWP 11 (NWP 5-01).

An OPORD is an operations plan made up of the heading, body, and ending. The basic plan, contained in the body of the OPORD, is concise and contains minimum detail. More detailed information on various ship departments is contained in enclosures (called annexes and appendixes).

The annex of most concern to radiomen is the communications annex. The communications annex, along with its appendixes and tabs, discusses the many details to be considered in planning communications for a particular operation. In this annex, you can find such information as the applicable circuits, equipment, and frequencies that will be used in the upcoming operation.

STANDARD OPERATING PROCEDURES

In addition to the OPORDs, you should also become familiar with the standard operating procedures (SOPs) used by your division and department. SOPs should be sufficiently complete and detailed to advise personnel of routine practices. The detail depends upon such variables as the state of training, the complexity of the instructions, and the size of the command.

Staff sections, divisions, and departments often find it convenient to establish their own SOPs for operating their respective areas and for guiding their personnel in routine matters. Some examples of communications SOPs are:

- Procedures for persons going aloft;
- Handling of visitors in radio spaces; and
- MINIMIZE procedures.

Communications SOPs are written to meet an objective. SOPs may vary from command to command and may differ according to their objectives. Your job will be to recommend changes or maybe even write the objectives. In any event, a complete set of SOPs will enable you and your shipmates to perform your duties in a responsible, professional, and safe manner.

MESSAGE LOGS

Accounting for messages addressed to your guard list (list of commands for which you receive message traffic) is the most important part of processing messages. Accounting for all messages processed in your message center is accomplished with logs. Although ashore and afloat automated systems automatically log, store, and retrieve messages, there still is a need to manually log and file both incoming and outgoing messages.

CENTRAL MESSAGE LOG

Depending upon the traffic volume processed, a message center may use either a separate outgoing/incoming log or a combined Central Message Log to record processed message traffic. All messages are logged in the Central Message Log after they have been logged in the appropriate circuit log. The normal practice is to use separate logs for outgoing and incoming messages (figure 2-5).

The entries in the Central Message Log are station serial number (SSN), precedence, DTG (original on a readdressal), originator (original on a readdressal), subject, classification, time of receipt (TOR) for incoming messages or time of delivery (TOD) for outgoing messages for each message. It is also useful to indicate on the log over which circuit the message was relayed. This is helpful during tracer situations. The Central Message Log is filed in the communications center master file on top of the messages processed for that radio day (raday).

TOP SECRET CONTROL LOG

Upon receipt of a Top Secret message, including SPECAT SIOP-ESI, addressed to the parent command or subscriber of the message center, the center assigns a sequential number and enters the originator, DTG, and copy count of the message into the Top Secret Control Log. A separate entry is made for each addressee. The messages must be annotated as "Copy ___ of ___" and "Page ___ of ___." The message must also be assigned a Top Secret control sequential number.

CIRCUIT LOGS

Records of messages sent via ship-shore circuits, whether primary shipshore, full-period termination, and soon, must be maintained. This ensures continuity of traffic, accurate times of delivery/receipt, and precise files for possible tracer action. These actions should be recorded on the Received Message Record, OPNAV

DATE _____

CENTRAL MESSAGE LOG

OUTGOING / INCOMING

SSN	PREC	DTC	ORIG	SUBJ	CLASS	TOR	TOD	CKT

RMJA0012

Figure 2-5.—Central Message Log for outgoing and incoming messages.

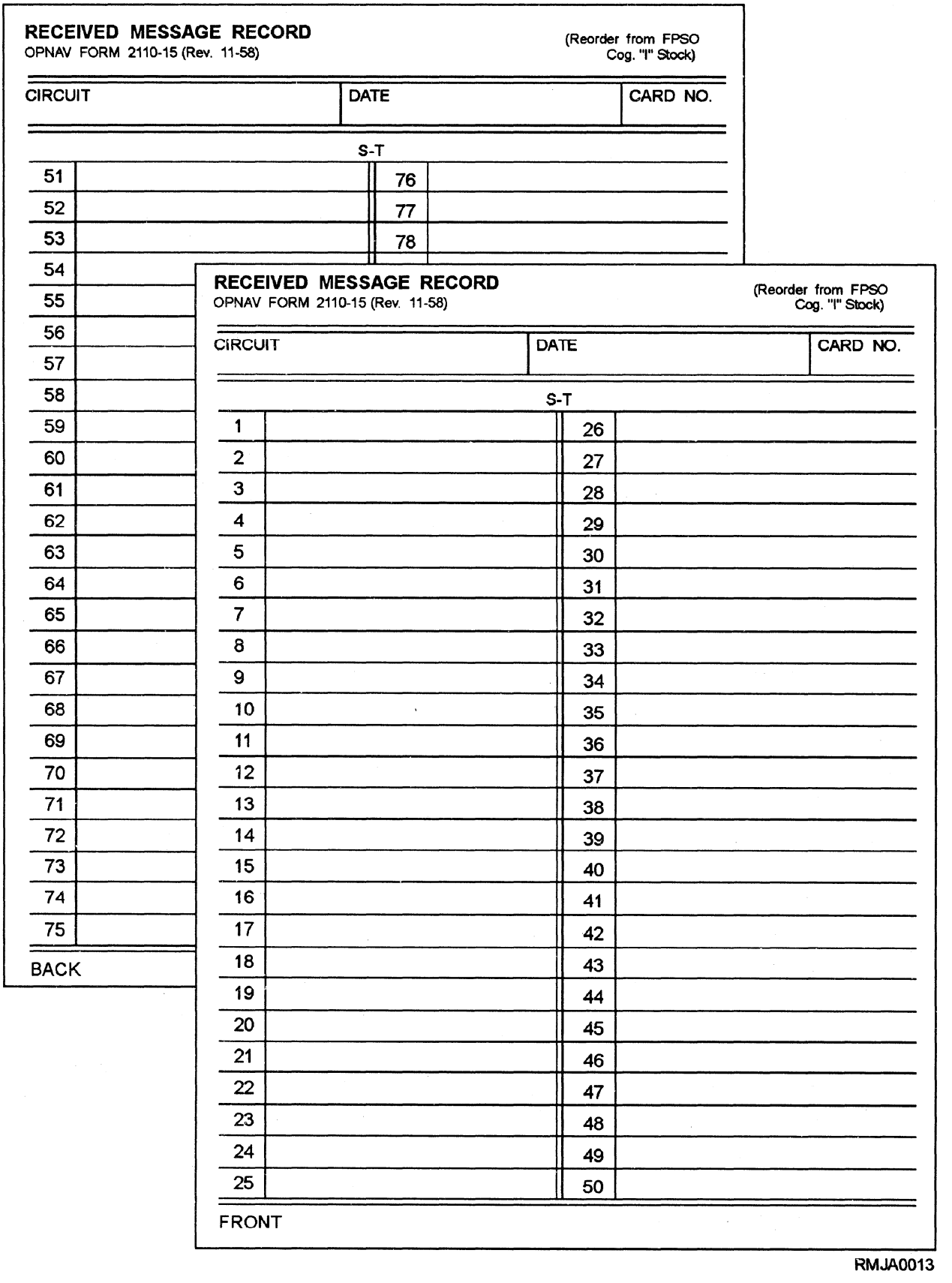


Figure 2-6.—Received Message Record, OPNAV Form 2110-15.

Form 2110-15 (figure 2-6). Although this form is primarily designed as a record of received messages, only a pen-and-ink change is necessary for its use as a send log.

JOURNAL LOGS

In most automated systems, all significant system events are entered in a journal log. This log is a chronological record of data processing operations, which may be used to reconstruct a previous or updated version of a file.

All system-level commands entered by an operator are logged. Log entries are usually queued for delivery to a printer as they are generated, but this is optional. However, they are always journaled to a file from which they can be recalled and printed at a later time, as desired. This log gives a system operator or supervisor the ability to review current and previous system events.

In addition, the journal log supports message accountability. The system records the receipt of every formal message and the termination of every formal message delivery that it schedules.

PROCESSING OUTGOING MESSAGES

Outgoing messages are those messages originated by:

- The command;
- Commands served by the communications center;
- An afloat command if a flag officer is embarked;
- An addressable unit onboard the ship as well as all messages accepted for relay.

The flow chart in figure 2-7 shows the actions required to process outgoing messages.

HANDLING AUTOMATICALLY PROCESSED OUTGOING MESSAGES

Those messages introduced into the LDMX/NAVCOMPARS from a PCMT, VDT, paper tape reader, data speed reader (DSR), card reader, or magnetic tape are considered "outgoing." They are prepared in JANAP 128, modified ACP 126, or other acceptable formats. Most outgoing messages are destined to be delivered to distant communications centers and commands. Others also have delivery requirements for in-house distribution to commands

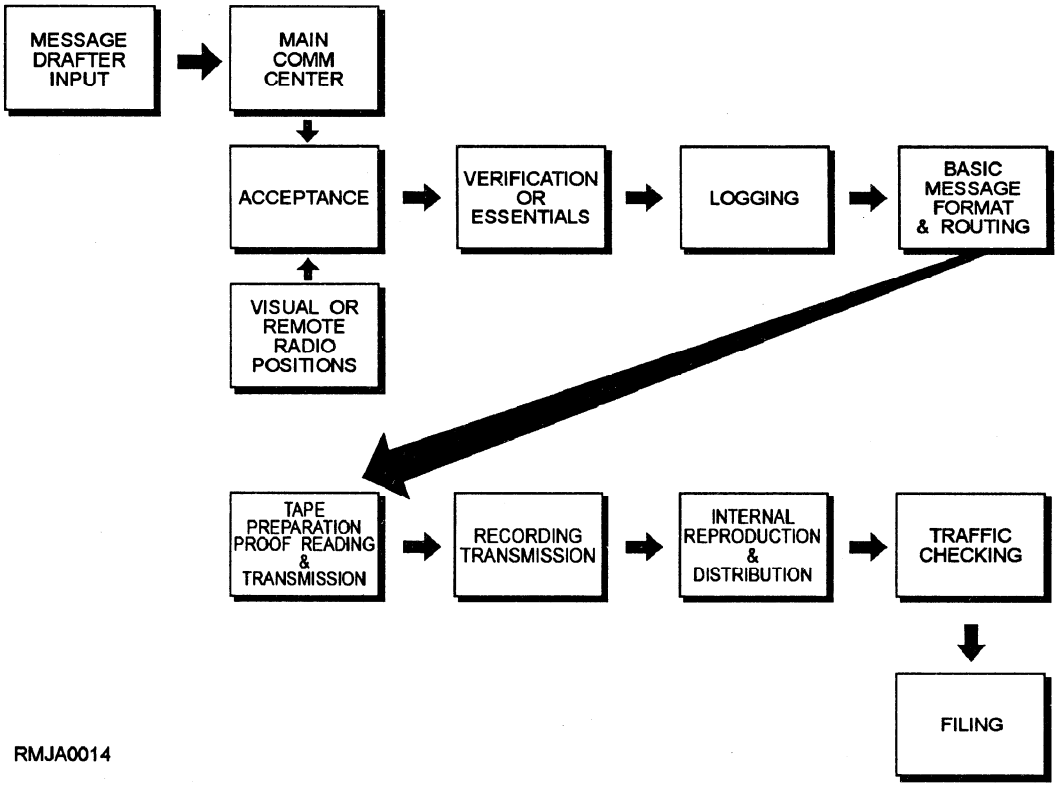


Figure 2-7.—Steps for processing outgoing messages.

serviced by the communications center. The basic steps for processing outgoing messages are shown in figure 2-8.

The system recognizes whichever format is used upon entry and then validates the start-of-message and end-of-message. After validation, the system outputs either an accept or a reject notice to the operator via the outgoing log. Together with the action notice, the system then outputs a unique header line to identify the message. Accepted messages are assigned a Process Sequence Number (PSN), which is included in the accept notice. They are then stored on diskette for recovery purposes and queued for processing on a first-in, first-out basis by precedence order.

Emergency command or FLASH precedence messages cause any lower precedence messages to be interrupted and a cancel transmission (bust) sequence to be transmitted. The emergency command or FLASH message is transmitted, and normal message processing by precedence is resumed.

Messages are selected for processing based on their precedence and on the order they arrived into the system; first ones in are the first ones processed out. The LDMX/NAVCOMPARS validates the message header and assigns routing indicators (RIs) for delivery as required.

If the system cannot assign an RI automatically, it will display the addressee line to the router VDT. The router may assign the correct RI, place the message on a queue, reject the message from further processing, or correct the short title of the addressee if in error.

A system status containing accounting information pertinent to all the messages on a hold queue will be displayed to the router via the VDT, when the router queue is empty or upon demand by the operator. The router can then retrieve any message on the hold queue by its PSN. If the router rejects the message, the system will record it and print a reject notice on the service log.

Any message determined by the LDMX/ NAVCOMPARS system to be duplicated will be rejected to the service printer with the proper annotation.

After all routing is appended to the message, the system assigns the language and media format (LMF)

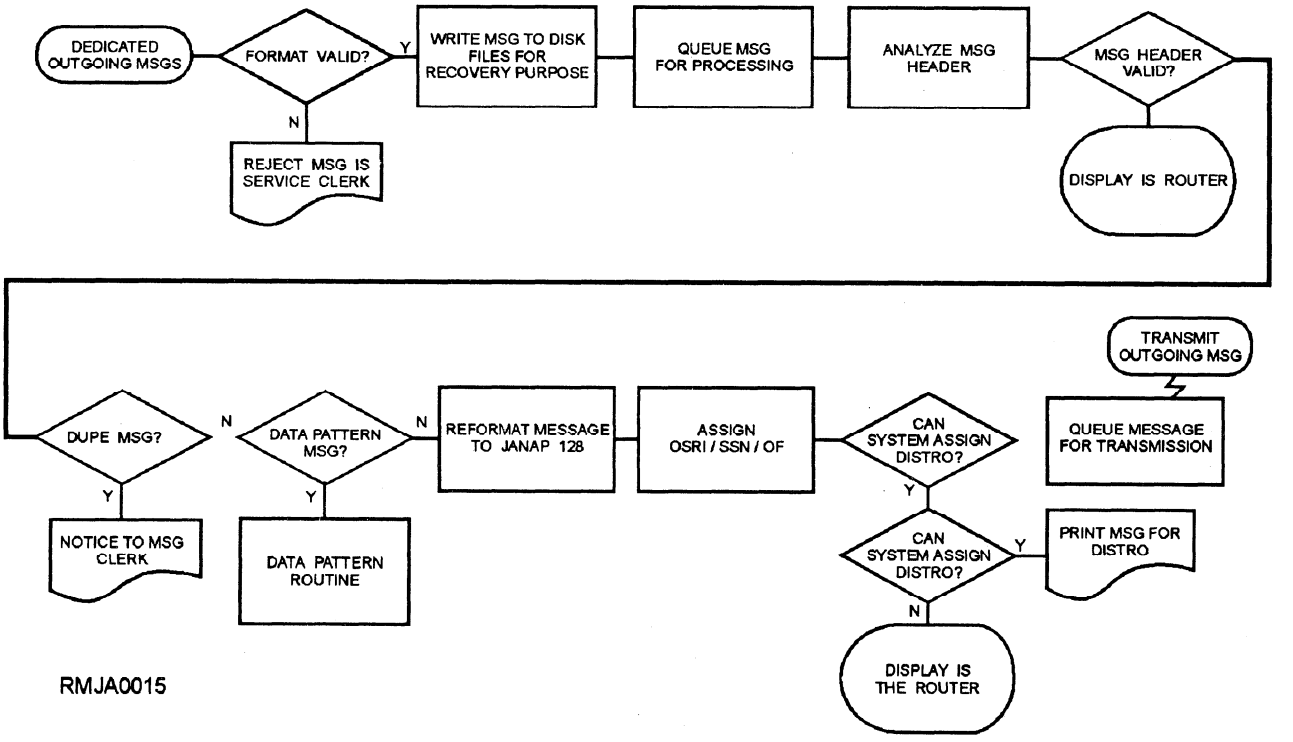


Figure 2-8.—Steps for processing automatic outgoing messages.

(JANAP 128), content indicator code (CIC) (JANAP 128), originating station routing indicator (OSRI), station serial number (SSN), and time of file (TOF) to the message. The message is then paged and sectioned according to JANAP 128, and queued for transmission.

Data-pattern messages may be introduced into the system via card or magnetic tape. The format will be in accordance with JANAP 128 procedures for data messages. During the message preparation, processing, transmission, and filing, the same controls and restraints used for narrative message processing will also apply to data-pattern messages.

The message may also have delivery requirements for distribution to commands serviced by the communications center. The system will automatically assign internal message distribution for all guard commands. If the system cannot provide internal distribution, the message will be displayed to the inrouter for assistance.

MESSAGE AND ROUTING ADDRESSEES

Most messages have at least one addressee responsible for taking action on the contents and for originating any necessary reply. Addressees who have an official concern in the subject of the message, but who do not have primary responsibility for acting on it, receive the message for information. Although information addressees are usually concerned only indirectly with a message, they occasionally must take action of some kind within their own commands. Some messages contain only information addressees.

Messages may be divided into types, according to the way they are addressed, as follows:

Single-Address— A message that has only one addressee, which may be either for action or information.

Multiple-Address— A message that has two or more addressees, which may be either action or information and where each addressee is informed of all other recipients.

Book— A message destined for two or more addressees but where the drafter considers it unnecessary that each addressee be informed of other addressee(s). Book messages are routed according to each addressee's relay station. All unnessary addressees are deleted from the face of the message before being sent to the addressee(s) served by that particular relay station.

General Message— A message that has a wide, predetermined, standard distribution. General messages are normally titled with a sequential number for the current year; for example, ALCOM 28/96, NAVOP 30/96. The title indicates distribution and serves as the address designator.

ADDRESS GROUPS

Address groups are four-letter groups assigned to represent a command, activity, or unit. In military communications, address groups can be used in the same manner as call signs to establish and maintain communications. Generally speaking, the Navy uses address groups the same way as call signs. Address groups never start with the letter N; hence, they are easily distinguishable from naval radio call signs. Address groups, however, follow no distinctive pattern, and the arrangement of the four letters that constitute them conveys no significance whatsoever.

Afloat commands (except individual ships) and shore-based commands or activities not served by their own communications facilities are assigned address groups. For example:

- Senior commands and commanders ashore, such as the Secretary of Defense and the Secretary of the Navy;
- Navy bureaus, systems commands, and district commandants; and
- Elements of the shore establishment having a need for direct addressing and receipt of message traffic (such as weather centrals).

Among other uses, address groups facilitate delivery of message traffic when a communications center serves so many activities that its own call sign is insufficient to identify the addressee. Address groups are contained in *Allied Call Sign and Address Group System—Instructions and Assignments,* ACP 100, and in *U.S. Call Sign &Address Group System Instructions & Assignments (U.S. Supplement No. 1),* ACP 100 U.S. SUPP-1. Like call signs, address groups are divided into the following types:

- Individual activity;
- Collective;
- Conjunctive;
- Geographic;
- Address indicating; and

- Special operating.

Individual Activity Address Groups

Individual activity address groups are representative of a single command or unit, either afloat or ashore. For example:

DTCI—COMNAVSURFLANT; and
SSMA—CHIEF OF NAVAL OPERATIONS (CNO).

Collective Address Groups

Collective address groups represent two or more commands or activities. Included in this group are commanders and their subordinate commanders. For example:

JTBC—DESRON 6; and
YQHV—SUBRON 16.

Conjunctive and Geographic Address Groups

Conjunctive and geographic address groups are discussed together because they are interrelated in their usage.

Conjunctive address groups have incomplete meanings and must have geographic address groups added to them to denote a specific command or location. For this reason, conjunctive address groups are used only with one or more geographic address groups. For example, the conjunctive address group XZKW means "All ships present at ___ ." To complete the meaning, it must be followed by a geographic address group.

Geographic address groups are the equivalent of geographical locations or areas. They are always preceded by conjunctive address groups. For example, the address group DEXL could represent Newport, R.I. Therefore, all ships present at Newport would be addressed XZKW DEXL.

Address Indicating Groups

Address indicating groups (AIGs) represent 16 or more specific and frequently recurring combinations of action and/or information addressees. The purpose of AIGs is to increase the speed-of-traffic handling. They shorten the message address by providing a single address group to represent a large number of addressees. This eliminates individual designators for each address used in the heading.

Messages that are repetitively addressed to a constant group of 16 or more addressees can effectively be processed by an AIG address designator. For example, let's assume that a hypothetical AIG (AIG 31) is used to address SUBMISS/SUBSUNK message traffic by COMSUBLANT to 30 action addressees and 35 information addressees. Since a single AIG (AIG 31) is used, 65 call signs and address groups are eliminated from the heading of the message.

AIGs are normally created when particular types of message traffic become repetitive enough (at least 12 times a year) and are addressed to enough of the same addressees to warrant it. Among such message traffic are:

- Alerts, air defense warnings, operational or emergency actions, and so forth;
- Destructive weather warnings, such as hurricanes and typhoons;
- Logistical transactions and reports;
- Intelligence summaries;
- Movement reports, such as aircraft, ships, and personnel; and
- Notices to airmen (NOTAMs).

A point for you to remember is that an AIG will not be established for groups of addressees numbering fewer than 16. A complete listing of AIGs by number, cognizant authority, and purpose is contained in *U.S. Navy Address Indicating Group (AIG) and Collective Address Designator (CAD) Handbook*, NTP *3* SUPP-1. A partial listing of AIGs, along with specific action and information addressees, can be found in ACP 100 U.S. SUPP 1.

Special Operating Groups

Special operating groups (SOGs) are four-letter groups that are identical in appearance to address groups. SOGs are provided for use in the headings of messages to give special instructions. However, SOGs are not used unless specifically authorized by CNO. They must always be encrypted. SOGs may be used singly or with encrypted or unencrypted call signs or address groups.

DISTRIBUTION CLERK

The distribution clerk reproduces copies of the messages according to the routing instruction of the inrouter and outrouter. The distribution clerk is responsible for making the required number of copies

each subscriber requires and slotting the messages into the appropriate subscriber box.

It is important that the clerk remain alert to prevent slotting messages into the wrong box. This could cause an undelivery situation. The distribution clerk, who handles a great number of messages throughout the watch, must be aware of high-precedence messages and ensure that they are reproduced and distributed in a timely manner for immediate pickup by the subscriber. The clerk must also be "up" on the message center's current SOP for handling special and classified messages.

To prevent viewing by unauthorized personnel, certain messages, such as PERSONAL FOR, AMCROSS, and classified messages, must be placed in envelopes for pickup by subscribers.

Classified messages are placed in two envelopes; the inner envelope is stamped with the classification and any special-handling markings, and then sealed in accordance with local instructions. The outer envelope is marked with the addressee, originator, and DTG of the message, and then sealed.

After reproducing and distributing a message, the distribution clerk places the original copy into a box for filing by the file clerk. When a message is reproduced from the sole copy of a broadcast message, the original copy or a filler must be returned to the broadcast file. If two-ply paper is used on the circuit, the top copy may be used as the master file copy and the bottom copy retained as the circuit monitor copy.

COMMON MESSAGE ELEMENTS

Before covering the basic format of military messages, we will first discuss the time system and precedence categories used in naval communications.

TIME

Time is one of the most important elements in communications. Messages are normally identified and filed by either date-time group or Julian date, depending on the method of transmission.

Date-Time Group

The date-time group (DTG) is assigned for identification and file purposes only. The DTG consists of six digits. The first two digits represent the date, the second two digits represent the hour, and the third two digits represent the minutes. For example, 221327Z AUG 96 means the 22nd day of August plus the time in Greenwich mean time (GMT). The dates from the first to the ninth of the month are preceded by a zero. We will talk more about the GMT system shortly.

The DTG designation is followed by a zone suffix and the month and year. The month is expressed by its first three letters and the year, by the last two digits of year of origin; for example, 081050Z AUG 96. The zone suffix ZULU (Z), for Greenwich mean time, is used as the universal time for all messages. The exception is where theater or area commanders prescribe the use of local time for local tactical situations. Radiomen never use 2400Z and 0000Z as the DTG of a message. The correct time would be either 2359Z or 0001Z, as appropriate.

GREENWICH MEAN TIME.— In naval communications, the date-time group is computed from a common worldwide standard. To meet the need for worldwide time standardization, the international Greenwich mean time (GMT) system was developed. The GMT system uses a 24-hour clock instead of the two 12-hour cycles used in the normal civilian world.

In the GMT system, the Earth is divided into 24 zones. Zone zero lies between 7 1/2° east and 7 1/2° west of the 0° meridian. The 0° meridian passes through Greenwich, England. The time in this zone (zone zero) is called Greenwich mean time (GMT). The military more commonly refers to this as **ZULU** time. Both names refer to the same standard.

Each time zone extends through 15° of longitude. Zones located east of zone zero are numbered 1 through 12 and are designated minus. To obtain Greenwich mean time, you must **subtract** the zone number in which you are located from local time.

Zones located west of zone zero are also numbered 1 through 12 but are designated plus. These zones must be **added** to the local zone time to obtain GMT. As we will discuss shortly, the 12th zone is divided by the 180th meridian, which is the international date line.

Each zone is further designated by a letter. Letters A through M (J is omitted) designate the eastern, or minus, zones. Letters N through Y designate the western, or plus, zones. The designating letter for GMT is Z (ZULU). The zone number, prefixed by a plus or minus sign, constitutes the zone description. Zones crossing land areas often follow boundaries, natural features, or regional demarcations to keep similar or closely related areas within the same zone.

CONVERTING GMT AND LOCAL TIMES.— Most countries have adopted the GMT system. As a Radioman, you will need to be able to convert local time to GMT. To do this, you must understand the GMT system. Figure 2-9 is a chart showing the time zones of the world. Refer to the chart as you study the material in the next paragraphs.

To illustrate converting local time to GMT, assume that we are in zone R and the local time is 1000R (10 a.m.). Referring to the time chart in figure 2-9, you can see that zone R lies west in longitude from zone zero, and is designated plus 5. Therefore, we add 5 hours to the local time, 1000, to find that GMT is 1500Z. To convert GMT to local time, we reverse the process and subtract 5 hours from the GMT (1500Z) to obtain 1000R.

The U.S. military services use the 24-hour system to express time in four-digit groups. The first two digits of a group denote the hour and the second two digits, the minutes. Thus, 6:30 a.m. becomes 0630; noon is 1200; and 6:30 p.m. is 1830. Midnight is expressed as 0000 (never as 2400), and 1 minute past midnight becomes 0001. Remember, to eliminate any possible confusion, never use 0000Z or 2400Z as the date-time group of a message. The correct time would be either 2359Z or 000IZ.

We mentioned earlier that the 12th zone is divided by the 180th meridian. This meridian is the international date line (IDL) (figure 2-9). This is where each worldwide day begins and ends. A westbound ship crossing the line loses a day, whereas an eastbound ship gains a day. This time zone is divided into literal zones MIKE and YANKEE. The eastern half of zone 12 is designated MIKE (-12), and the western half is designated YANKEE (+12).

Now we come to a very important point in our discussion. Since MIKE and YANKEE are two parts of a single zone, the time in MIKE and YANKEE is <u>always</u> the same. When the IDL is crossed from either direction, the day must change. Since we have already established that there is a l-hour difference between each of the 24 time zones, it is clear that there is always a situation where it is a day earlier or later in one part of the world than it is in another. The primary point to remember about this zone is that it is always the same time in zone MIKE as it is in zone YANKEE, but it is <u>never</u> the same day! You can find more information on time zones in *Communication Instructions General (U),* ACP 121.

Julian Date

The Julian date consists of seven digits. The first three digits represent the day, and the last four digits represent the hour and minutes. The first day of the calendar year is Julian 001, and each day is numbered consecutively thereafter. For example, in Julian 0311315, 031 is the 31st day of the calendar year (January 31), and 1315 is the filing time.

PRECEDENCE

The message drafter indicates the desired writer-to-reader delivery time (speed-of-service) through the assignment of a message precedence. Although the drafter determines the precedence, the releaser should either confirm or change it. (We will talk more about the responsibilities of the drafter, originator, and releaser later in this chapter.)

Precedence is assigned according to urgency, based solely on speed-of-service, not according to the importance of the subject matter or the text. For example, an unclassified message may be assigned an IMMEDIATE precedence, whereas a Secret message may be assigned a ROUTINE precedence. In this situation, the unclassified message requires fast action or response, whereas the Secret message may not require any action at all.

The following paragraphs list the various precedence categories, their indicators, and basic definitions:

ROUTINE (R)— This category is assigned to all types of traffic that justify electrical transmission but which are not of sufficient urgency to require a higher precedence.

PRIORITY (P)— This category is reserved for messages that furnish essential information for the conduct of operations in progress. This is the highest precedence normally authorized for administrative messages.

IMMEDIATE (O)— This category is reserved for messages relating to situations that gravely affect the national forces or populace and which require immediate delivery to addressees.

FLASH (Z)— This category is reserved for initial enemy contact reports or operational combat messages of extreme urgency; message brevity is mandatory.

YANKEE (Y)— In addition to the four major precedence categories, an EMERGENCY COMMAND PRECEDENCE (ECP) is used within the

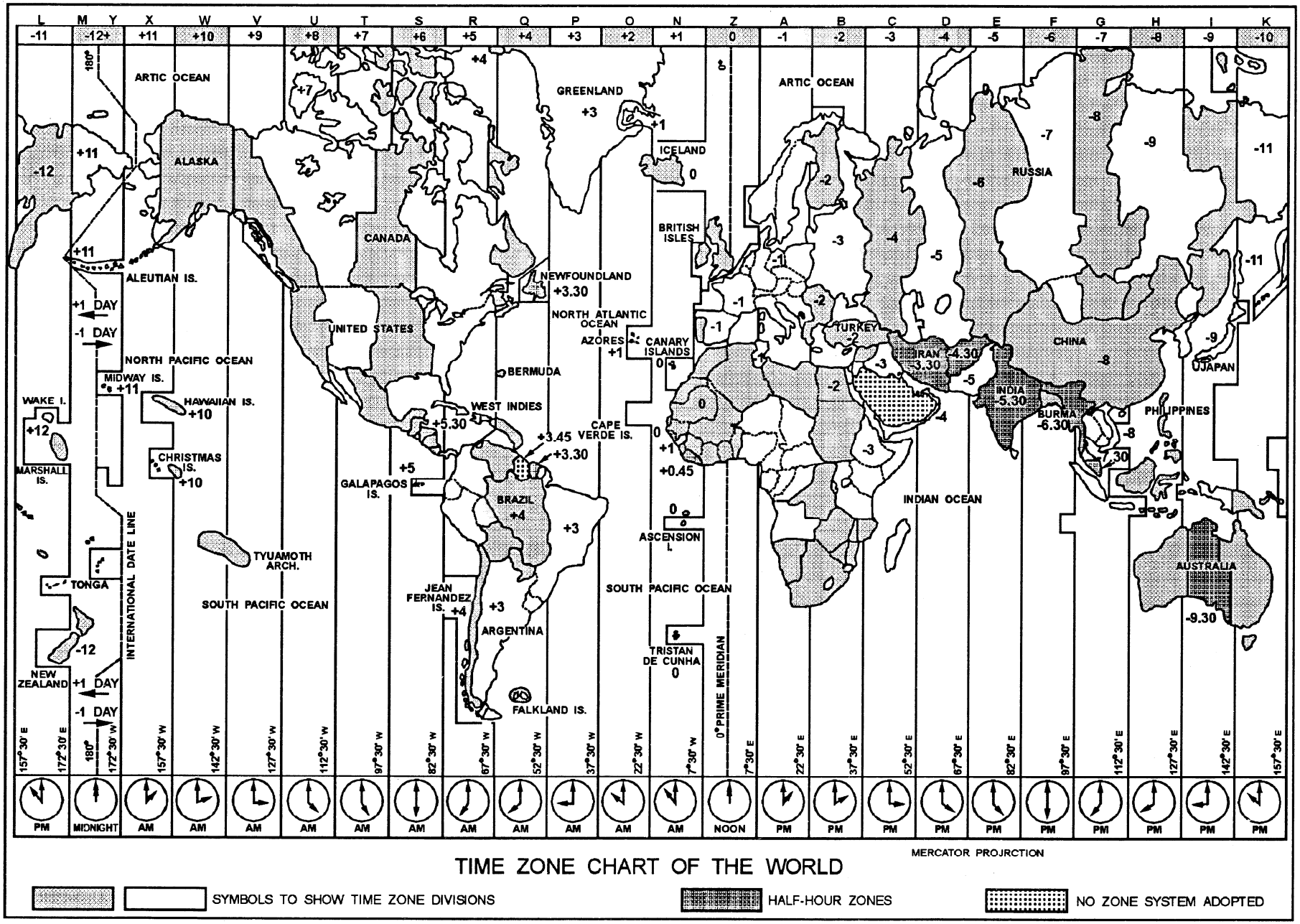

L M Y X W V U T S R Q P O N Z A B C D E F G H I K
-11 -12+ +11 +10 +9 +8 +7 +6 +5 +4 +3 +2 +1 0 -1 -2 -3 -4 -5 -6 -7 -8 -9 -10
ARTIC OCEAN
GREENLAND
ICELAND
ALASKA
CANADA
BRITISH ISLES
RUSSIA
ALEUTIAN IS.
NEWFOUNDLAND
NORTH ATLANTIC OCEAN
UNITED STATES
AZORES
CANARY ISLANDS
TURKEY
IRAN
CHINA
JAPAN
NORTH PACIFIC OCEAN
MIDWAY IS.
BERMUDA
INDIA
PHILIPPINES
WAKE I.
HAWAIIAN IS.
WEST INDIES
BURMA
CAPE VERDE IS.
MARSHALL IS.
CHRISTMAS IS.
GALAPAGOS IS.
BRAZIL
INDIAN OCEAN
ASCENSION
TYUAMOTH ARCH.
AUSTRALIA
TONGA
SOUTH PACIFIC OCEAN
JEAN FERNANDEZ IS.
ARGENTINA
TRISTAN DE CUNHA
NEW ZEALAND
FALKLAND IS.
INTERNATIONAL DATE LINE
0° PRIME MERIDIAN
+1 DAY
-1 DAY
157°30' E 172°30' E 180° 172°30' W 157°30' W 142°30' W 127°30' W 112°30' W 97°30' W 82°30' W 67°30' W 52°30' W 37°30' W 22°30' W 7°30' W 7°30' E 22°30' E 37°30' E 52°30' E 67°30' E 82°30' E 97°30' E 112°30' E 127°30' E 142°30' E 157°30' E
PM MIDNIGHT AM AM AM AM AM AM AM AM AM AM AM NOON PM PM PM PM PM PM PM PM PM PM
MERCATOR PROJRCTION
TIME ZONE CHART OF THE WORLD
SYMBOLS TO SHOW TIME ZONE DIVISIONS
HALF-HOUR ZONES
NO ZONE SYSTEM ADOPTED
RMJA0016

Figure 2-19.—Time zone chart of the world.

AUTODIN system. This ECP is identified by the precedence prosign Y and is limited to designated emergency action command and control messages.

MESSAGE USER RESPONSIBILITIES

A message user is any individual authorized to draft, release, and/or process electronically transmitted messages. There are certain responsibilities associated with the origination of a message. These responsibilities are separate and distinct and concern the following parties:

- Originator;
- Drafter; and
- Releaser.

Occasionally, the responsibilities may overlap, especially if one person is serving a dual capacity. For example, communications officers may occasionally draft and release messages, thus making them both drafters and releasers.

ORIGINATOR

The originator is the authority (command or activity) in whose name the message is sent. The originator is presumed to be the commanding officer of the command or activity. Most often, the originator and the releaser are one and the same.

In some cases, the drafter, releaser, and originator are all the same person. For example, if the commanding officer drafts a message for transmission, he or she is the drafter as well as the releasing authority for the activity in whose name the message is sent.

DRAFTER

The drafter is the person who actually composes the message. In accordance with NTP 3, the drafter is responsible for:

- Proper addressing and using plain language address (PLA) designators correctly;
- Clear, concise composition;
- Selecting the precedence;
- Ensuring the proper format;
- Assigning the proper classification; and
- Ensuring the application of proper downgrading and declassification instructions to classified messages, except those containing Restricted Data or Formerly Restricted Data.

RELEASER

The releaser is a properly designated individual authorized to release messages for transmission in the name of the command or activity. The releasing individual ensures that the drafter has complied with the requirements contained in NTP 3. In addition to validating the contents of the message, the signature of the releaser affirms compliance with message-drafting instructions. The signature of the releaser authorizes the message for transmission.

After a message has been properly released, it is delivered to the telecommunications center (TCC) for transmission. The DTG is normally assigned here. Proper transmission, receipting, and filing procedures are done by the communications personnel.

An important point that you should remember about the DTG is that it is assigned for identification and file purposes only. It is not used to compute message processing time.

MESSAGE READDRESSALS

If you receive or send a message and later determine that another activity may need to act on or know about the information in the message, you can readdress the original message to that activity. If you receive a copy of a message as an "information addressee," you can only readdress the original for information purposes.

Use a short form or long form, depending on how long ago the original message was sent. For both the short form and long form, you must:

- Fully identify the message you are readdressing.
- Enter the new addressee(s).
- Enter the original message originator.
- Include the original date-time group.
- Use the Process Sequence Number (PSN), if contained in the original message.

If the original message was sent within the last 60 days, use the short form to readdress it. Messages are held in the message center file for up to 60 days. On the short form, enter the *from, to,* and *information addressees* in the fields provided. Send the short form to the message center where it will be combined with the text of the original and then sent.

The short form readdressal is always unclassified. However, it must state the classification of the readdressed message.

Messages over 60 days old are routinely deleted from the message center files. If the original message to be readdressed is more than 60 days old, use the long form. Enter the *from, to,* and *information addressees* in the fields provided. Unlike the short form, you retype the entire message. Classify the long form the same as the original message.

When a sectionalized message is readdressed, each section of the message must be readdressed separately. The headerlines and addressees must be the same on each readdressal. The PSN must match that of the section being readdressed, but the respective section number is omitted. Each section of the readdressed message should have the same date-time group.

The precedence of the readdressal message maybe lower, the same as, or of a higher precedence than the original message when deemed operationally imperative by the readdressal authority.

General formatting instructions and preparation guidance are available in NTP 3. Message readdressal procedures may vary slightly at different TCCs. The required procedure may be verified through the local TCC.

MINIMIZE MESSAGES

Military telecommunications systems tend to become overloaded during an emergency. Naturally, it becomes necessary to reduce unnecessary traffic volume to clear user circuits for essential traffic. This reduction in traffic is accomplished by use (usually by message) of the word "MINIMIZE." Minimize means **"It is now mandatory that normal message and telephone traffic be reduced drastically so that vital messages connected with the situation indicated will not be delayed."**

A message ordering minimize consists of the word "MINIMIZE" followed by the area affected (scope), reason, and duration of the minimize condition (when known). Minimize messages must be brought to the immediate attention of the leading communications petty officer (LPO) and the communications officer.

The Chief of Naval Operations (CNO), fleet commanders in chief, and area coordinators are authorized to impose minimize conditions on users of naval communications systems. Subordinate commanders may impose minimize over elements of their commands only with prior permission from one of the three authorities just mentioned.

During minimize conditions, FLASH and IMMEDIATE traffic should be restricted to a maximum of 100 and 200 words, respectively. Message releasers are also kept to a minimum and must be specifically designated in writing. We briefly discuss additional minimize guidelines later in this chapter. NWP 4 (NWP 6-01) contains information pertaining to the types of normal, environmental, and supply traffic that may be sent over normal channels and circuits during minimize.

SERVICE MESSAGES

Service messages are short, concise messages between communications personnel. These messages have the authority of an official communication and must receive prompt attention. If the action requested in a service message cannot be accomplished within a reasonable time, the station originating the service message should be notified. Service messages are normally assigned a precedence equal to the message being serviced.

Service messages deal with many topics. You will find that most deal with corrections, repetitions, broadcast reruns, and misrouted or missent messages. You must remember that a service message should be promptly dealt with and retained until all actions concerning it have been completed. Once action is complete, it is good practice to attach a copy of the service message to the serviced message when it is filed, or mark it with the DTG of the service(s).

Requests for information through service messages should be as brief, concise, and accurate as possible. Careful attention to detail and the use of proper operating techniques by communications and crypto personnel will reduce the number of service messages required.

Service messages are normally prepared in abbreviated plaindress format and may be assigned sequential reference numbers. (We discuss plaindress messages later in this chapter.) The service message number immediately follows the abbreviation "SVC" in the message text. If used, sequential service reference numbers may continue throughout the calendar year. When you reply to a service message received with a reference number, the text of the reply should refer to the number. For example:

```
UNCLAS SVC //N00000// ZUI SVC 0245 RUEDCSA1234 1921600
```

This example is a service message inviting attention (ZUI) to a previous service message with a reference number of 0245. Occasionally, you will see the acronym COSIR in a service message text, which means "Cite Our Service in Reply." Authorized operating signals are used to the greatest extent possible in service messages, but clarity must not be sacrificed for brevity.

The security classification is the first word of all service message text. This is followed by the abbreviation "SVC." If the service message requires special handling, the special-handling designator follows the security classification. For example:

UNCLAS SVC or SECRET SPECAT SIOP ESI SVC

A service message may quote the textual content of a classified message or refer to the classified message in a manner that reveals textual content. In this case, the service message must be assigned the same classification as the classified message being serviced. You can find detailed information on service messages in *Automatic Digital Network (AUTODIN) Operating Procedures,* JANAP 128.

Tracer Messages

Tracer messages are special types of service message. Tracers are sent to determine the reason for excessive delay or nondelivery of a message previously sent. Normally, tracer requests are initiated by a message originator or addressee. However, a situation may dictate that tracer action be initiated by the originating communications station, the relay station, or the communications station of the addressee.

Tracer action continues on a station-to-station basis until the cause of delay has been determined. Upon receipt of a tracer, a station should examine its records for the time of receipt and transmission of the message being traced. This information is compiled and transmitted with the tracer action to the preceding station(s) and to the station that originated the tracer. The station that caused the delay or nondelivery must cite the reason and provide a summary of corrective action in the report.

Tracer action requests must be initiated as soon as the discrepancy is discovered. Action must be initiated no later than 4 days after the original time of transmission for a tactical addressee. For nontactical addressees, action must be initiated no later than 30 days from the original time of transmission. In-station records, files, logs, and tapes must be retained beyond the required retention limit if tracer action is in progress prior to the expiration date. You can find detailed information concerning tracer action in JANAP 128.

Termination Request Messages

Ships send termination request messages to establish circuits with a NCTAMS or NAVCOMTELSTA on a limited or full-time basis. A termination request message must be sent to the cognizant NCTAMS at least 48 hours prior to activating the requested termination. If the ship has a requirement for a full-time termination, it will be assigned a routing indicator by the cognizant NCTAMS. NTP 4 contains detailed information pertaining to termination requests and formats.

Communications Guard Shift Messages

Communications guard shift (COMMSHIFT) messages are required when a command shifts its guard from one broadcast or servicing communications center to another. When possible, the shift takes effect at 0001Z of the new radio day. When broadcasts are shifted, an overlap period before and after the effective time is observed to ensure continuity of traffic. The command guards both broadcasts during the overlap period.

COMMSHIFT messages are sent to the NCTAMS of the communication areas from which the old and the new broadcasts originate. COMMSHIFT messages are necessary because of operational considerations or changes in the deployment schedule of a ship. These messages are necessary when a command needs to effect a shift at a time other than that indicated by its movement report. Detailed information concerning communications guard shift messages and formats is contained in NTP 4.

Broadcast Screen Requests

Broadcast screen requests (BSRs) are service messages to request the rerun (ZDK) of missed or garbled messages. BSRs are sent to the Broadcast Keying Station (BKS) or to the designated broadcast screen ship that is responsible for the broadcast channel. NTP 4 provides detailed information and prescribes proper format for drafting a BSR.

COMMSPOT Reports

COMMSPOT reports are used to advise of any situation that might cause significant disruption of

tactical communications. These reports are submitted by all ships and nonterminated units when unusual communications difficulties are encountered. COMMSPOT reports must be submitted as soon as unusual communications difficulties are experienced to minimize further deterioration of the communications situation.

COMMUNICATIONS CENTER FILES

Every message handled by a ship or communications station is placed in one or more files. Some files are maintained by all ships and stations. Other files are optional and are maintained only to fill the needs of a particular ship or station.

COMMUNICATIONS CENTER MASTER FILE

The communications center master file is the heart of the filing system. This file contains a copy or filler of every message sent or received by your command. Messages or fillers must be filed in DTG order to facilitate speed in locating messages. Those messages not having DTGs should be filed behind messages of the same date. Separate incoming and outgoing communications center master files maybe maintained.

CRYPTOCENTER FILE

The cryptocenter file contains a copy of each Top Secret, SPECAT (less SIOP-ESI), and messages designated for special privacy, regardless of classification. Tight Control (TICON) and NATO messages must have their own files. Fillers for messages in this file must be placed in the master station file.

SPECAT SIOP-ESI FILE

The SPECAT SIOP-ESI file contains the master copy of all SIOP-ESI messages received by the communications center. Fillers for these messages must be placed in the master station and cryptocenter files.

BROADCAST FILE

The broadcast file contains a copy or filler of each message transmitted or received by the broadcast method. This file must be stored in accordance with the highest classification of the information contained. Top Secret and SPECAT messages addressed to the command must be filed in their appropriate files and a filler for these messages placed in the broadcast file.

STATION FILE

The station file is divided into two parts: communications center master file and visual station file. With the exception of broadcast messages, the master file contains the circuit or "as is" copy, including any message endorsements, of all messages transmitted, received, or relayed by the communications center. Narrative visual messages or fillers must be filed in the communications center master file.

GENERAL MESSAGE FILE

The general message file contains copies of all effective general messages that require retention based on the communications center's current guard list. This file is subdivided by general message title (such as ALNAV, ALCOM, NAVOP), and messages are filed in serial number order instead of DTG order. An example of a general message serial number is ALNAV 10/96. This indicates that it is the 10th ALNAV sent in 1996.

The individual file is marked with the classification of the highest classified message contained therein. The classified files may be segregated by security classification if desired. If a general message is canceled during the current year, the message may be destroyed, but a filler must be placed in the file to identify and indicate the disposition of all current-year general messages.

FACSIMILE FILE

The facsimile file contains a copy of all transmissions processed by facsimile equipment. A filler for all facsimile messages must be placed in the communications center master file.

COMMERCIAL TRAFFIC FILE

The commercial traffic file contains messages sent by commercial systems in accordance with *Fleet Communications (U),* NTP 4. This file is maintained by the commercial traffic clerk.

EMBARKED COMMAND FILE

The embarked command file is maintained by the embarked commander's staff. When embarked commanders depart their flagships, they may require

that their files accompany them. Therefore, the embarked command file is maintained separately from the flagship file. Flagship communications personnel are responsible for processing outgoing and incoming messages for the embarked staff.

NATO/ALLIED FILES

Classified messages of foreign origin must be provided the same protection as U.S. messages of equivalent classification. Foreign Restricted messages, for which there is no U.S. equivalent, must be protected the same as U.S. Confidential messages, except that Restricted messages do not have to be stored in a security container. You can find U.S. equivalent and foreign classifications in the *Department of the Navy Information and Personnel Security Program Regulation,* OPNAVINST 5510.1, hereinafter called the *Security Manual.*

NATO classified messages may not be filed with U.S. classified message. However, NATO classified message files may be stored in the same storage area with U.S. messages provided that the NATO files are clearly marked as such.

FILE FILLERS

Because of repeated reference to previously sent message traffic, you must be able to locate all messages easily and quickly. Therefore, you must always return a message to the same file from which it was removed and in the proper filing order. When you remove a message from a file, always insert a filler, or tickler, in its place.

Fillers are locally prepared forms that identify the message by the original DTG, the message originator, information as to where the message is located, and the personal sign of the person removing the message from the file and completing the filler. For readdressal messages, a filler is made for each readdressal date-time group. The message itself is filed under the original date-time group. Figure 2-10 shows an example of a message filler, or tickler.

FILE MAINTENANCE

Messages and fillers are filed in ascending date-time group order. The earliest message of the radio day (raday) will be at the bottom of the file. Automated systems print the DTG of each message on the lower right-hand corner of each message. For messages processed on nonautomated systems, the DTG should also be printed on the lower right-hand corner. This aids personnel in easily locating messages in the files. When a message is removed from a file, it is important that it be refiled as soon as possible.

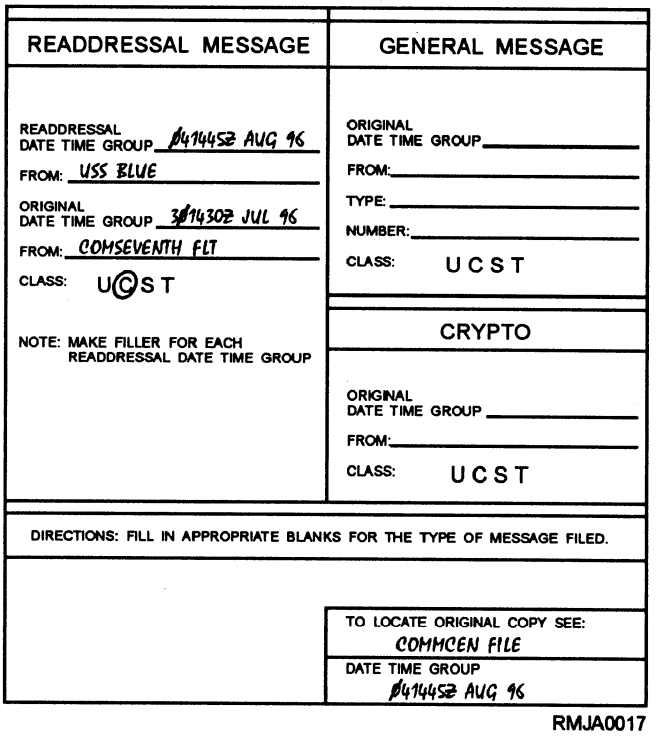


Figure 2-10.—Example of a message filler.

The importance of maintaining well-kept files and of moderating among the various watch sections cannot be overemphasized. Maintaining accurate files and records and observing proper procedures contribute to an efficient shipboard or shore communications organization. You should be aware that different ships and stations may do basic procedures in slightly different ways. All commands, however, must conform to the requirements contained in communications operating instructions and publications.

RETENTION OF FILES

Communication logs and files are retained by a communications center for a specified time period, as shown in table 2-1. After the time period indicated, the logs and files should be destroyed either by burning or shredding. Because of the volume of message traffic processed, logs and files can take up significant space in the message center; therefore, they should be destroyed in a timely manner.

Table 2-1.—Retention Period of Logs and Files

FILE/LOG	RETENTION PERIOD
Broadcast	24 Hours
Card	30 Days
Central message log	30 Days
Circuit (teleprinter)	5 Days
Commercial traffic	12 Months
Communications center master (Either paper or LDMX/NAVCOMPARS journal tapes)	30 Days
Cryptocenter file	2 Years
Cryptocenter destruction log	2 Years
Facsimile	60 Days
General Message	When Canceled
Intelligence summaries	10 Days
Messages incident to distress or disaster	3 Years
Messages incident to or involved in any complaint for which the command has been notified	2 Years
Messages of historical or continuing interest	Permanently
Meteorological maps and summaries	2 Days
Monitor rolls and message tapes	24 Hours
SPECAT SIOP-ESI file	60 Days
TOP SECRET control log	60 Days
Watch-to-watch inventory	30 Days

COMMUNICATIONS PLANNING

The primary objectives of communications planning are:

- To provide for effective connectivity to support the exercise of command and the exchange of essential information; and
- To advise the commander of the implications of communication capabilities and limitations for the operation plan and its execution.

The communications plan has to consider reliability, security, and speed. The communications planner chooses facilities and methods that will best satisfy operational requirements. The plan provides for the command and control capability by which the operation will be controlled and directed.

To be effective, the communications planner needs comprehensive knowledge of the organizational structure established for the operation and the capabilities and limitations of the communications and command center facilities available to the force.

COMMUNICATIONS REQUIREMENTS

The operational tasks assigned to various units require radio nets that link units engaged in the same activity or task. Communications circuits follow the command lines of the task unit or contribute to its tactical effectiveness by providing for essential information exchange. These considerations provide the essential elements for determining communications requirements.

PROTECTION OF COMMUNICATIONS

Enemy interception and disruption of communications are of primary concern to any communications planner. Every facet of communications facilities, methods, and procedures needs to be examined in terms of security, vulnerability to deception, and the electronic protection (EP) required for maximum protection.

Communications Security

Security is the safeguarding of information. As it pertains to communications, security is usually referred to in terms of communications security (COMSEC) and signal security (SIGSEC). Security will be discussed in more depth in chapter 3. Various devices and procedures are used to increase security, including:

- **Authentication—** A security measure designed to protect communications systems against acceptance of false transmissions or simulations by establishing the validity of a transmission, message, or originator.
- **Codes—** Any system of communication in which arbitrary groups of symbols represent units of plain text. Codes are often used for brevity and/or security.
- **Ciphers—** Any cryptologic system in which arbitrary symbols or groups of symbols represent units of plain text.
- **Radio Silence—** A condition in which all or certain radio equipment is kept inoperative (frequency band and/or types of equipment are specified).
- **Monitoring—** The act of listening, carrying out surveillance on, and/or recording the emissions of one's own or allied forces for the purpose of maintaining and improving procedural standards and Security.
- **Identification Friend or Foe (IFF)—** A system using electromagnetic transmissions to which equipment carried by friendly forces automatically responds. For example, by emitting predetermined IFF pulses, friendly forces can distinguish themselves from enemy forces.

Communications Deception

Communications deception, part of the field of tactical deception, is the use of devices, operations, and techniques with the intent of confusing or misleading the user of a communications link or a navigation system.

EA and EP

Electronic attack (EA) is that division of electronic warfare (EW) involving actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. Enemy EA concerns the communications planner because overcoming enemy jamming and deception imposes certain restrictions on general communications operations procedures.

Electronic protection (EP) is that division of EW involving actions taken to ensure friendly effective use of the electromagnetic spectrum despite an enemy's use of electronic warfare. The planner must be aware of EP capabilities available.

THE COMMUNICATIONS PLAN

The communications plan satisfies the communications requirements of an operation. It specifies circuits, channels, and facilities to be used and stipulates the policies and procedures that are applicable. The plan is, in effect, an assignment of communications tasks to be performed by subordinate commanders or by supporting commands.

The planner first establishes requirements for communications and then determines the best means for satisfying them. This process may reveal shortages or inadequacies in what is available. If inadequacies are identified, it may become necessary to share circuits or facilities, as well as merging or consolidating requirements. All possibilities should be considered to support valid operational requirements.

In planning communications, the planner must evaluate such factors as the performance, capabilities, and capacities of systems, facilities, and personnel. These factors are merely guides and averages. They represent the sum result of experience in previous similar situations, and are considered only after any local factors are determined. These factors change from time to time and must all be available for final determination of communications requirements.

TELECOMMUNICATIONS SERVICE REQUEST (TSR)

When a command requires additions, deletions, or changes in existing Defense Communications System (DCS) circuits, it must initiate a TSR. The submission of a TSR is not a simple process and requires research and planning. The Defense Information Systems Agency (DISA) publishes a publication called *Submission of Telecommunications Service Request*, DISA CIRCULAR 310-130-1, that provides instructions for preparing and submitting TSRs. New, increased, or updated services are expensive and require substantial justification.

The increasingly high cost of telecommunications support, especially leased services, has resulted in the high visibility of communications programs at all levels of government. This fact underscores the need for managerial awareness and improved life cycle documentation of telecommunications resources.

Planning and developing a responsive naval telecommunications system requires early identification and consideration of user requirements. Programming is required to obtain necessary resources. Normally, these requirements should be defined and submitted at least 2 years in advance to permit timely system planning and programming.

TELECOMMUNICATIONS SERVICE ORDER (TSO)

The TSO is the authorization to start, change, or discontinue circuits, trunks, links, or systems. It is used to amend previously issued TSOs and to effect administrative changes.

The basic circuit design information for all new or changed circuits will be provided by the TSO. The TSO may also be used as the authority to procure specific devices and ancillary equipment necessary to install the circuit or services designated.

FREQUENCY MANAGEMENT

Over the last quarter century, electronics has pervaded virtually every facet of our life. High-tech electronic devices, especially those that radiate, make constant use of the electromagnetic spectrum.

The term “electromagnetic spectrum” refers to the natural vibrations that occur when a force is applied to a substance. These vibrations occur with various speeds and intensities. The speed at which they occur is called frequency, and the distance between each vibration is called wavelength. Frequency and wavelengths are discussed in a later module.

Spectrum Management

A great invention in the 19th century ultimately led to the need for spectrum, or frequency, management. This invention was the wireless or, as we know it today, the radio. At first, there were only two radio frequencies—50 kilohertz (kHz) and 1000 kHz. Today, the spectrum is recognized by international treaty to extend up to 3000 gigahertz (GHz). The development of radar, satellites, and other technologically advanced systems and their subsequent demands on the frequency spectrum have contributed to the need for frequency management.

Frequency Allocation

The Department of the Navy will obligate no funds for equipment until a frequency allocation has been obtained. This means that all actions necessary to establish a frequency band for a specific item must be completed and approved prior to budgeting funds.

The allocation approval authority considers the type of service the item will provide and the classification of the emission. This authority also enforces rules and regulations and compliance with technical standards. The approval authority also ensures the compatibility of emerging equipment with other equipment operating in the same electromagnetic environment.

Interservice frequency coordination is another important consideration. It reduces the potential for harmful inteference if more than one service develops similar items that will operate in the same band. The coordination is the responsibility of the Chief of Naval Operations (CNO), working through the United States Military Communications Electronics Board (USMCEB).

Frequency Assignment

Frequency assignment is the process of authorizing a system or equipment to operate on a discrete frequency (or frequencies) and within a specified set of constraints. Examples of constraints are power, emission bandwidth, location of antennas, and operating time.

Authority for using radio frequencies by Navy and Marine Corps activities within the United States and

Possessions (US&P) is obtained from the Administrator, National Telecommunications and Information Administration (NTIA), Washington, D.C.

The CNO establishes overall policy for spectrum management within the Department of the Navy. Authority for using radio frequencies by Navy and Marine Corps activities within the area of responsibility of a unified or specified commander is obtained from the Joint Chiefs of Staff through the USMCEB. Within the Department of the Navy, the Naval Electromagnetic Spectrum Center (NAVEMSCEN) authorizes frequency assignment applications and ensures all prerequisites are completed.

SPECIAL-HANDLING MARKINGS

Certain types of messages require special-handling markings in addition to that provided by the security classification. Among these markings are such designations as Caveat, Restricted Data (RD), Formerly Restricted Data (FRD), LIMDIS, FOUO, EFTO, SPECAT, PERSONAL FOR, NATO RESTRICTED, and ALLIED RESTRICTED.

Caveat Messages

When used with special-handling instructions, the word "caveat" means a warning by authoritative orders that directs or imposes one to protect an element, usually special message traffic.

Restricted Data and Formerly Restricted Data

The marking "Restricted Data" (RD) is applied to all data concerned with the design, manufacture, or use of nuclear weapons. Also included in this category is the special nuclear material used in energy production.

The marking "Formerly Restricted Data" (FRD) pertains to defense information that has been removed from the RD category but must still be safeguarded as classified defense information. FRD material cannot be released to foreign nationals except under specific international agreement.

LIMDIS (Limited Distribution)

The LIMDIS designator is applied only to classified messages which, because of the subject matter, require limited distribution within the addressed activity.

For Official Use Only (FOUO)

FOUO is the designation used on official information not requiring a security classification but which must be withheld and protected from public release. Unclassified messages containing FOUO information must have the abbreviation "FOUO" after the designation "UNCLAS."

Encrypt for Transmission Only (EFTO)

Certain categories of unclassified messages may be identified as having potential value if subject to analysis, but do not meet the criteria for security classification. The special designation "EFTO" was established to protect these unclassified messages during electrical transmission.

EFTO is not required on unclassified messages addressed exclusively among Navy, Marine Corps, and Coast Guard commands. EFTO is authorized for use within the Department of Defense, including the National Security Agency. However, EFTO is required on FOUO messages addressed to DOD activities outside the continental United States. Bear in mind, however, that just because information is FOUO, it is not automatically EFTO, and vice versa.

As we mentioned earlier, EFTO is a transmission marking for unclassified messages. FOUO markings, however, define a certain category of information requiring special handling. Neither FOUO nor EFTO markings are security classifications; both are special-handling designations. You can find detailed information on EFTO and FOUO markings in *Basic Operational Communications Doctrine (U),* NWP 4 (NWP 6-01).

SPECAT

The SPECAT marking means special category. SPECAT messages are classified messages identified with a special project or subject. SPECAT messages require special-handling procedures in addition to the handling procedures for the security classification of the message. There are four SPECAT categories:

- SPECAT;
- SPECAT EXCLUSIVE FOR (SEF);
- SPECAT Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI); and
- PSEUDO-SPECAT.

SPECAT and SPECAT EXCLUSIVE FOR messages must be at least Confidential. SPECAT SIOP-ESI messages are always Top Secret. PSEUDO-SPECAT messages are normally unclassified messages that require limited distribution. Examples of PSEUDO-SPECAT messages include AMCROSS messages, urinalysis test results, and HIV test results.

SPECAT messages are handled only by those personnel who are authorized by the commanding officer in writing to view them. The types of information assigned SPECAT and handling procedures can be found in NWP 4 (NWP 6-01) and in *Fleet Communications (U)*, NTP 4, respectively.

PERSONAL FOR

PERSONAL FOR is the marking applied when message distribution must be limited to the named recipient. Only flag officers, officers in a command status, or their designated representatives may originate PERSONAL FOR messages.

NATO RESTRICTED

The United States does not have a security classification equivalent to NATO RESTRICTED. NATO messages classified as restricted must be safeguarded in a manner similar to FOUO messages. Messages originated by NATO must be handled in accordance with *NATO Security Procedures (U)*, OPNAVINST C5510.101.

ALLIED RESTRICTED

The United States does not have a security classification equivalent to ALLIED RESTRICTED. However, these messages must be handled in the same manner as Confidential messages. U.S.-originated messages containing ALLIED RESTRICTED information are marked as "Confidential" immediately following the security classification.

MINIMIZE CONSIDERED

During an actual or simulated emergency, it may become necessary to decrease the amount of record and/or voice communications on military telecommunications circuits. When this occurs, it is called MINIMIZE. In essence, all messages that are not urgent will not be transmitted. Those messages that concern a mission or safety of life are considered imperative and, therefore, require transmission during minimize.

The same criteria pertaining to minimize conditions noted earlier in this chapter still apply. The releasing officer must review and decide on the message's merit, which means the message will be sent, either electrically or by another means. When a message is released, it must include the words "MINIMIZE CONSIDERED" and "RELEASED BY."

Messages that will not be sent electrically during minimim periods should be returned to the originator with the reason for their return. Normally nontransmitted messages will be sent via U.S. mail if they meet established security guidelines.

JCS EMERGENCY ACTION MESSAGES

Joint Chiefs of Staff (JCS) Emergency Action Messages (EAMs) contain key instructions or information from high-level authority and have predetermined formats (pro forma). Such messages are transmitted by various communications systems and normally carry FLASH (Z) precedence. They are vital messages of an extremely time-sensitive nature, and rapid processing is mandatory to achieve the fast reaction required by their content. Usage and handling procedures are issued by the JCS to those who have a need to know.

SPECAT messages come in two variations. One type includes both the general SPECAT and the SPECAT Single Integrated Operational Plan—Extremely Sensitive Information (SPECAT SIOP-ESI). This type of SPECAT message is associated with code words or projects. For example, a Secret message whose subject matter deals with a special project entitled "TACAMO" would have a classification line reading SECRET SPECAT TACAMO. SPECAT SIOP-ESI messages are always classified Top Secret. SPECAT (less SIOP-ESI) messages must be classified at least Confidential.

The other type of SPECAT message is SPECAT EXCLUSIVE FOR (SEF). SEF is used only within the naval community for highly sensitive matters, high-level policy, or when politically sensitive information is to be passed only to a particular individual. The classification line would then contain the name of that individual. For example, a Secret message destined exclusively for Admiral W. T. Door would read:

SECRET SPECAT EXCLUSIVE FOR ADM W. T. DOOR //N00000//

SEF messages are reserved for use by flag officers and officers in a command status. These messages are not intended for use in operational matters, and they

may not be readdressed nor referenced in other narrative messages.

SPECAT messages are handled only by those personnel who are authorized to view them as approved in writing by the commanding officer.

NAVAL WARFARE PUBLICATIONS LIBRARY

The naval warfare publications library (NWPL) is the designation assigned to that group of communications and operational publications designated as part of the publication allowance for the command. These publications contain required procedures, signals, and other information of an operational or mission-essential nature. They may also include information involving safety. The NWPL provides for the central administration and maintenance of communications and operational publications. These publications include, but are not limited to:

- Naval telecommunications publications (NTPs);
- Naval warfare publications (NWPs);
- Fleet exercise publications (FXPs);
- Allied tactical publications (ATPs);
- Allied exercise publications (AXPs);
- USN addenda to allied publications; and
- Miscellaneous allied publications.

The objective of central administration of naval warfare publications (NWPs) is to ensure that these publications are correct and readily available for their intended use. Some NWPs contain information that is necessary for the proper performance of individual duties and is important for individual professional development. Therefore, NWPs must be readily available for use by individuals with a duty-related need or a general professional need for the information.

NAVAL WARFARE PUBLICATIONS CUSTODIAN

The responsibility for managing the NWPL is assigned to an officer or senior petty officer who is responsible to the executive officer, department head, or division officer. This assignment is a collateral duty, and the person assigned is known as the naval warfare publications custodian (NWPC). This person is responsible for the overall administration and security of the NWPL in accordance with the *Naval Warfare Documentation Guide,* NWP 0 (NWP 1-01).

NAVAL WARFARE PUBLICATIONS LIBRARY (NWPL) CLERK

The NWPL clerk is a person assigned by the NWPC. The clerk is responsible for the upkeep and maintenance of the library. The NWPL clerk maintains all records and receipts in the central file, orders all necessary publications and changes thereto, and enters all changes and amendments to publications physically held in the NWPL. The clerk reports all matters of concern to the library custodian.

NWPL ADMINISTRATION

The NWPL custodian issues publications to holders and short-term users. A holder is a person who has permanent subcustody of a publication under the central control of the NWPL. The holder is responsible for maintaining the publication, entering all changes and amendments, and providing adequate security. A user is a person who checks out a publication for temporary or short-term custody.

Signature custody and disclosure records for classified material are maintained as required by the Security Manual. Signature custody of unclassified publications is not required. However, the records of the NWPL should provide an up-to-date location of publications that have been issued to holders or checked out to users. Where signature custody is not required, a locator card maybe used in place of a catalog card to check out publications to users.

NWPL MAINTENANCE

Several basic files are used in maintaining the NWPL. One is the custody file, which contains a NWPL Catalog Card, OPNAV Form 5070-11 (figure 2-11), for each naval warfare publication on allowance or on board. The purpose of this file is to maintain an up-to-date record of the holder and location of each publication. This record also helps keep track of entries and changes to the publication. The catalog card can also be used as a custody card and as a destruction record. When used as a record for security purposes, it must be retained as required by the *Security Manual.*

The administrative file, sometimes called the transaction file, contains designation letters for custodian, local allowance/inventory sheets, the directives file, responsibility acknowledgment forms,

SHORT TITLE	COPY Documents On Hand	CLASSIFICATION OF PUBLICATION
NTP 4( )	m 1 p 2 3 4 5 6	
LONG TITLE		EFFECTIVE DATE

CHANGE OR CORRECTION	DATE OF ENTRY BY COPY NUMBER									
	1	2	3	4	5	6	7	8	9	10
CHG #1										
CHG #2										
MSG CORR 1/1										

NOTES: MSG CORR entered into a microfiche copy of a publication be placed into the envelope with the copy and annotated on the envelope.

ENTRY DATE will be written into each column for each copy of the publication receiving change or correction.

OPNAV FORM 5070-11 (11-57) BACK

DEPOSITION OF PUBLICATION						
COPY NO.	HOLDER (Signature)	LOCATION	REC'D. DATE	RETURN DATE	DESTRUCTION DATE	DESTRUCTION AUTHORITY
1&2	NWPL Custodian's Sig	NWPL	*1		*5	*6
1	Subcustodian's Sig	RADIO	*2	*3		
		CENTRAL				
1	NWPL Clerk's Sig	NWPL	*4			

NOTES: *1. Date copy received into library.
*2. Date subcustodian received copy.
*3. Date subcustodian returned copy to library.
*4. Date publication received by library.
*5. Date copy destroyed.
*6. Authority cited for destruction of copy.

RMJA0018

Figure 2-11.—NWPL Catalog Card.

publication notice route slips, destruction records, inspection documentation letters, and copies of all correspondence pertaining to naval warfare publications. Included in the administrative file is the Change Entry Certification form, OPNA 5070/12, shown in figure 2-12. This form is filled out by the holder of the applicable publication. Material in the administrative file must be retained for 2 years.

NWPL BINDERS

Binders for U.S. naval warfare publications are color-coded according to their security classification. The color codes are RED for Secret, YELLOW for Confidential, and BLUE for unclassified. Allied/NATO publications have white binders regardless of security classification.

CHANGE ENTRY CERTIFICATION
OPNAV 5070/12 (REV. 6-75)

RETURN TO NAVAL WARFARE
PUBLICATIONS LIBRARY

SHORT TITLE	COPY NO.	CHANGE	EFFECTIVE DATE

REMARKS:

I certify that the above change or correction has been entered and the list of effective pages was checked against the contents of the basic publication, and the superseded pages and residue of the change were returned to the Naval Warfare Publications Library.

NOTE: *Missing pages or other defects should be reported in the REMARKS space above.*

SIGNATURE	ENTRY DATE

PART 2 S/N 0107-LF-050-7061

SHORT TITLE	COPY NO.	CHANGE	EFFECTIVE DATE

REMARKS:

I acknowledge receipt of the above change and certify that this change will be entered upon the effective date/immediately and that the superseded pages will be returned to the Naval Warfare Publications Library within five (5) working days thereafter.

SIGNATURE	DATE

PART 1 S/N 0107-LF-050-7061 C-3500

Figure 2-12.—Change Entry Certification form.

ENTRY OF CHANGES

The timely and accurate entry of changes to NWPL publications is necessary to ensure accurate, up-to-date information as well as information continuity. The NWPL clerk is responsible for making changes or corrections to NWPL publications or ensuring that holders receive. and make the changes in a timely manner.

Changes are often so numerous that all communications personnel may become involved in making them. The NWPL clerk is responsible for ensuring that all personnel making changes or corrections to NWPL publications know the proper procedures for making these changes. These procedures are a follows:

- Check the Foreword or Letter of Promulgation of the change for the effective date of the change/correction to ensure that the publication to be corrected is effective.
- Read all the specific instructions contained in the change or correction before making the entry.
- Use any dark ink EXCEPT RED for pen-and-ink entries. Red is not visible under red night lights used aboard ship.
- Type lengthy pen-and-ink corrections on a paste-in cutout. All superseded matter must be deleted in ink prior to inserting the cutout.
- Use flaps when no room exists for a cutout. When used, flaps should be attached to the binder side of the page.
- Use rubber cement or mucilage for pasting instead of glue or gummed tape.
- Make a notation in the margin adjacent to the entry after making pen-and-ink corrections, citing the source of the correction; for example, ALCOM 007/96.

After page changes are entered, a page check must be conducted and the page change and page check recorded on the Record of Changes and Corrections sheet.

Corrections to NWPL publications are issued by message when the material requires rapid dissemination. These numerical message corrections (NMCs) are normally sent as general messages. NMCs are assigned a two-number designation separated by a slant sign. The first number indicates the sequential number of the message correction to the original or revised publication. The last number is the printed change that incorporates the material. For example, NMC 7/3 is the 7th message correction and is incorporated into the publication by change 3.

PUBLICATION NOTICE

A publication notice gives a brief summary of a new publication or change. The notice is included with each hardback copy and is furnished solely for routing by the NWPC. These notices keep all cognizant personnel informed of the changes to naval warfare publications. The notices are destroyed when no longer useful.

WATCH-TO-WATCH INVENTORY

To ensure positive control of NWPL publications, a watch-to-watch inventory should be conducted. At the change of each watch, the watches jointly conduct a visual inventory of every publication held by the watch section. Those loose-leaf publications requiring a page check at the end of the watch must be indicated on the inventory sheet.

The signing of the watch-to-watch inventory by the relieving watch certifies that the publications were sighted, the required page checks were conducted, and that the relieving watch stander is responsible for them. Any discrepancies should be resolved prior to the relieving of the watch.

All signatures in the watch-to-watch inventory must be in ink. The inventory may be destroyed after 30 days if it is no longer needed for local reference. If watch-to-watch inventories are not required aboard ship, a daily inventory is required.

EXTRACTS

Naval warfare publications may be extracted/ reproduced for use in training or operations of U.S. forces. All extracts must be properly marked with the security classification and safeguarded in accordance with the Security Manual.

The classification assigned to an extract is the highest classification assigned to any article, paragraph, page, or pages from which the information is taken. Guidance for allied (NATO) publications is found in their NATO letters of promulgation.

RECEIVING NEW OR REVISED PUBLICATIONS

When new or revised publications are received, you should check the Foreword and the U.S. Letter of Promulgation for the effective status of the publication. The Foreword shows the effective status of the publication for allied usage; the U.S. Letter of Promulgation for U.S. use.

A revision to a publication can be issued that is effective for U.S. use but not for allied use. Particular care should be taken not to destroy the previous edition until the new revision is effective for allied use as well.

ALLIED COMMUNICATIONS PUBLICATIONS

With worldwide cooperation among friendly nations and the United States, the need arose for coordinated and standardized communications. To meet this need, the allied communications publications (ACPs) were developed. The ACP series provides communications instructions and procedures essential to conducting combined military operations and communications in which two or more allied nations are involved. A Radioman's work often requires familiarity with ACPs.

JOINT ARMY-NAVY-AIR FORCE PUBLICATIONS

Joint Army-Navy-Air Force publications (JANAPs) were developed to coordinate and standardize communications among the U.S. military services. The publication *Status of Noncryptographic JANAPs and ACPs,* JANAP 201, lists the short and long titles, content of each publication, and the current edition of JANAPs and ACPs.

NAVAL TELECOMMUNICATIONS PUBLICATIONS

Naval telecommunications publications (NTPs) are the main communications publications in use by the U.S. Navy, Coast Guard, and Marine Corps. The NTPs include information and guidance from basic communication information (NTP 4), to frequency spectrum management (NTP 6), and commercial traffic (NTP 9), just to name a few areas of communications.

NAVAL WARFARE PUBLICATIONS

Naval warfare publications (NWPs) incorporate the results of fleet tactical development and evaluation programs and fleet and allied (NATO) experience. NWPs also provide information about the tactical capabilities and limitations of equipment and systems. NWP 0 (NWP 1-01) provides guidance for managing the NWPL and lists the publications contained in the library.

FLEET TELECOMMUNICATIONS PUBLICATIONS

Fleet telecommunications publications (FTPs) are the guiding doctrine of a NCTAMS for the communications area under its jurisdiction. To provide optimum communications responsiveness to fleet requirements. FTPs incorporate the unique communications procedures for the COMMAREA into a standardized fleet-oriented procedural document. FTPs are based on the NTP series.

COMMUNICATIONS INFORMATION BULLETINS

Communications information bulletins (CIBs) are developed by each NCTAMS to provide reference information on specific tactical communications subjects. CIBs also provide communications operating personnel with communications procedural information applicable to a specific COMMAREA. NTP 4 lists the CIBs and their contents.

SUMMARY

As you have learned from this chapter, the naval communications establishment is quite complex. We communicate not only with other U.S. naval commands, both at sea and ashore, but also with other U.S. military services and allied nations. Before the messages that you send reach their destinations, they may travel through other networks in the Defense Communications System.

We have introduced you to the basic principles of communications management, evaluation of both personnel and the work area, and duties of individual positions within the command. We have also covered various categories of messages that have both internal and external use in the message center.

This chapter has introduced you to the standard procedures associated with handling incoming and outgoing messages. Because of the volume of messages a telecommunications center processes, it is essential that communications personnel observe all the handling procedures to prevent losing or delaying delivery of messages to subscribers.

Understanding the communication plan will give you a view of the ever-changing overall plans for your ship or shore station and its requirements for mission completion.

The various publications that you, as a communicator, rely on are continually being updated. Communications is an area that is constantly changing in areas of equipment and procedures. Therefore, it is important you become thoroughly familiar with all the publications and current changes that pertain to your communications area.

The tasks of a message center are extremely important. Your understanding of the handling procedures is key to providing fast and accurate communication to the fleet.

CHAPTER 3

COMMUNICATIONS SECURITY

LEARNING OBJECTIVES

Upon completing this chapter, you should be able to do the following:

- *Identify the procedures used in handling, inventorying, destroying, and setting up COMSEC equipment.*
- *Identify reports and forms associated with CMS reporting requirements.*
- *Identify the procedures and measures to be used with transmission security.*

As a Radioman, you will often deal with sensitive subject matter that requires special security handling. It is for this reason that we have communications security (COMSEC). Within the framework of COMSEC, we have directives and requirements that deal specifically with communications material.

COMSEC involves all the protective measures taken to deny unauthorized persons information derived from the possession and study of telecommunications relating to national security. COMSEC also consists of the measures taken to ensure the authenticity of our communications. COMSEC includes the following:

- Cryptosecurity, which results from measures taken to provide technically sound cryptosystems and their proper use;
- Physical security, which results from physical measures taken to safeguard COMSEC material and information;
- Transmission security, which results from measures designed to protect transmissions from interception and exploitation by means other than cryptoanalysis; and
- Emission security, which results from measures taken to deny unauthorized persons information derived from the interception and analysis of emanations from crypto and telecommunications equipments.

In this chapter, we will see how these elements of COMSEC are unique to the duties of a Radioman.

CRYPTOSECURITY

The Navy has instituted a unique distribution system to achieve technically sound cryptosystems. The Navy has also developed strict accountability and control procedures to ensure proper use of cryptosystems.

COMMUNICATIONS SECURITY MATERIAL SYSTEM (CMS)

The CMS is designed to ensure the proper distribution, handling, and control of COMSEC material and to maintain the cryptographic security of communications. Procedures governing the CMS can be found in *Communications Security Material System (CMS) Policy and Procedures Manual,* CMS 1.

CMS Account

Every command with a CMS account is assigned an account number by the Director, Communications Security Material System (DCMS). A command or activity with a CMS account number receives its COMSEC material directly from national and Navy sources. A CMS account command may also be responsible for COMSEC material transferred to other commands. The command assigns a CMS custodian

and alternates the responsibility for all overall management of the CMS account.

CMS Custodian and Alternate Custodians

The CMS custodian is the person designated in writing by the commanding officer to maintain the CMS account for the command. The alternate custodians are also designated in writing by the commanding officer and assist the CMS custodian.

In the custodian's absence, the alternates assume the duties of the custodian. Their duties include receiving, inventorying, destroying, and issuing COMSEC material and equipment to authorized users and local holders. They are also responsible for training all personnel involved in CMS and submitting required COMSEC reports to the proper authority in a timely manner. CMS 1 provides details on the responsibilities of the CMS custodian and alternates.

CMS Local Holder

A CMS local holder is a command or activity that receives its COMSEC material support from a CMS account command. The local holder command has a designated CMS custodian and alternates who are responsible to their commanding officer for the proper handling of COMSEC material and training of personnel involved. For example, if a ship drew all of its COMSEC material from a central account maintained by the squadron commander, the ship would have to be a local holder. Local holders must draw all of their material from only one CMS account and may not be local holders to two or more accounts.

CMS User

A CMS user is an individual who requires COMSEC material to accomplish an assigned duty or who needs COMSEC material for advancement study or training purposes. A CMS user must be properly cleared and authorized by the commanding officer to handle CMS material. As a Radioman, you will most likely become a user of COMSEC material.

CMS Witness

There may be times when you will be assigned as a CMS witness. You will be responsible for assisting a custodian or user in performing routine administrative tasks related to the handling of COMSEC material. As a witness, you must be familiar with applicable CMS procedures and command directives.

CMS Responsibilities

Whether you are a CMS user or a witness, you are responsible for the proper security, control, accountability, and destruction of CMS material in your workspace. Everyone involved with CMS material must comply with the procedures in CMS 1-related administrative and procedural publications. You must also comply with the CMS instructions of the command and higher authority.

CMS Training Requirements

The CMS custodian and alternates are responsible for training all personnel involved with COMSEC material in the proper handling, security, accounting, and destruction of COMSEC material. The CMS custodian may use the Personnel Qualifications Standards (PQS) for CMS as a training tool. All personnel who become involved with CMS should complete the PQS training course.

CMS Storage Requirements

COMSEC material must be stored separately from non-COMSEC material. This helps ensure separate control for COMSEC material and makes emergency destruction of COMSEC material easier. COMSEC material of different security classifications may be stored in the same security container drawer. COMSEC material, however, must be segregated according to classification so that it can be destroyed in a timely manner in an emergency.

Storage requirements for COMSEC keying material are more stringent than for nonkeying material. All COMSEC keying material requiring two-person integrity (TPI) must be stored in such a manner that a single person, including the CMS custodian, cannot obtain access. CMS 1 lists the storage requirements for COMSEC keying material.

Receipt

When COMSEC material is issued to a watch station, the area must be occupied and operated on a 24-hour, 7-day-a-week basis; an 8-hour, 5-day-a-week basis; or any similar basis (for example, combat information center (CIC)). COMSEC material received at a watch station must be signed for on a local custody document.

When you are on duty, the watch supervisor is responsible for all the COMSEC material listed on the watch-to-watch inventory. Additionally, any required page checks will be conducted prior to assuming responsibility for the listed COMSEC material.

Any inventory discrepancies found must be reported immediately to the CMS custodian or an alternate custodian in accordance with CMS 1 and also logged in the RADAY log.

CMS Inventory

Each time a watch section changes, the oncoming watch supervisor and a witness must inventory all COMSEC material held at a watch station. Two-person integrity must be maintained at all times during the inventory. When you inventory COMSEC material, you must do the following:

- Account for all keying material and page-check open keying packages;
- Visually inventory all COMSEC equipment and account for equipment by quantity; and
- Page-check all COMSEC publications.

The inventory sheet must list COMSEC material by short title, edition, and accounting number (if any). Both persons must sign the inventory sheet. CMS 1 outlines the requirements for inventorying COMSEC material.

COMSEC Material Accounting Reports

COMSEC material accounting reports provide an audit trail for all accountable COMSEC material. Reports may be prepared manually or be computer-generated. There are specific requirements for submitting all reports, including where they go and who they go to. These requirements are found in CMS 1.

The following reports are briefly described as to their general use. This list is not all-inclusive.

1. **Transfer Report—** Used to document and report the transfer of COMSEC material from one CMS account to another or one holder to another.
2. **Destruction Report—** Used to document or report the physical destruction of COMSEC material. The destruction must be witnessed by two appropriately cleared and authorized persons. The report must be completed immediately after the material is destroyed. Destruction reports are not normally submitted to DCMS unless directed to do so by DCMS.
   a. **Local destruction—** Destruction will be documented and retained locally using a SF 153, or a locally prepared equivalent form (CMS 25). Top Secret and Secret destruction reports must be kept for 2 years. Local destruction records are mandatory for all AL 1 and 2 COMSEC, regardless of classification, and optional for AL 3 and 4 COMSEC material classified Confidential and below.
3. **Receipt Report—** Used to document or report receipt of COMSEC material (usually used with a transfer report).
4. **Inventory Report—** Used to document and report the physical inventory of COMSEC material. There are three types of CMS inventories. Fixed-cycle (FC), Special, and Combined.
   a. Fixed-cycle inventory is to ensure that all accounts satisfy the national requirements for a semiannual inventory of keymat and an annual inventory of equipment and publications.
   b. Special SF 153 inventory is to satisfy the Navy requirement to conduct and document the mandatory Change of Command and Custodian inventories.
   c. Combined SF 153 inventory may sometimes be used for both the requirements for a Fixed-cycle inventory and a Special inventory.
5. **CMS 25 ONE-TIME KEYING MATERIAL DESTRUCTION REPORT—** This report is a two-sided document used to record destruction of individual, one-time keying material segments of COMSEC material. Side one is numbered 1-31 for daily use; the reverse side

explains the digraphs that are printed to the left of the short title on each segment of extractable tape (figure 3-1).

6. **CMS 25B COMSEC KEYING MATERIAL** LOCAL DESTRUCTION REPORT— The CMS 25B is a two-sided report used to record

CONFIDENTIAL (When Filled In)

CMS-25 ONE-TIME KEYING MATERIAL DESTRUCTION REPORT

Retain this form locally IAW Annex T, CMS 1. See Chapter 7, Art 790 for instructions on destroying one-time keying material

These individual one-time keying material cards or segments were destroyed on the dates and by the two individuals indicated below:

Card #	Date Extracted	Date Destroyed	Signature	Signature
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				

Short Title: Reg #/Accounting #: AL:

Formal destruction of the entire publication in accordance with CMS 1 on TN _____ dated _____

Grade/Signature _____ Grade/Signature _____

CLASSIFIED BY CMS-1

CONFIDENTIAL (When Filled In)

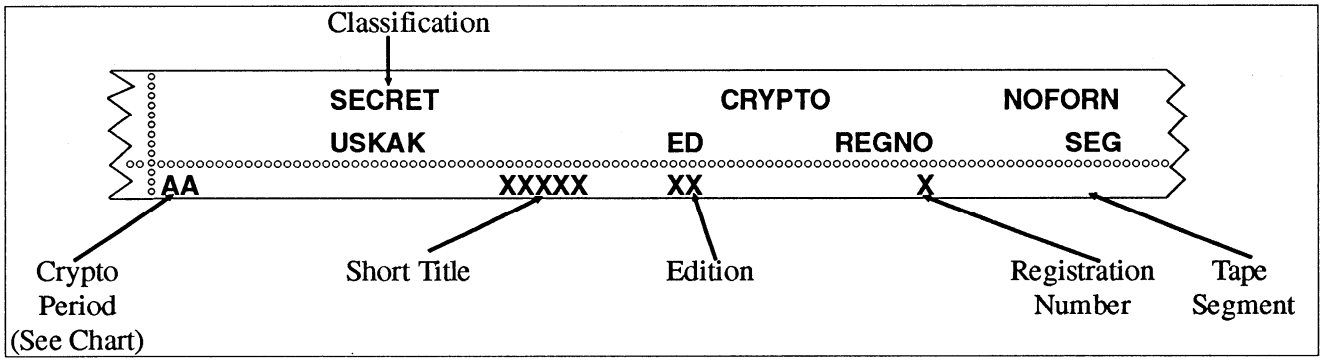
Figure 3-1A.—CMS-25 ONE-TIME KEYING MATERIAL DESTRUCTION REPORT (front).

CONFIDENTIAL (When Filled In)

Explanation of Keytape Crypto Periods

Number of Tape Segments				When to Change	
First Letter	# of Keys	# of Copies of Keys	Total Segments	Second Letter	Crypto Period
A	31	1	31	A	Daily [24 Hours]
B	5	3	15	B	Weekly [7 Days]
C	1	5	5	C	Monthly
D	6	5	30	D	Special [≤ 24 Hours]
E	5	1	5	E	No Prescribed Period
F	1	10	10	F	Three Months
G	16	1	16	G	Yearly
H	1	31	31	H	[Contact Controlling Authority]
I	1	15	15	I	Six Months
J	26	1	26	J	Monthly [Beginning 1st Day Used]
L	35	1	35		
M	2	1	2		
N	[Contact Controlling Authority]				
Q	34	1	34		
S	75	1	75		
T	12	1	12		
U	65	1	65		
V	62	1	62		
W	1	65	65		
R	4	5	20		
Y	26	2	52		
Z	15	5	75		

Example



CLASSIFIED BY CMS-1

CONFIDENTIAL (When Filled In)

Figure 3-1B.—CMS-25 ONE-TIME KEYING MATERIAL DESTRUCTION REPORT (back).

destruction of keytape segments of COMSEC keying material packaged in the "VF" format (62 unique segments per canister). Destruction of segments 1-31A must be recorded on the "A" side and segments 1-31B on the "B" side (figure 3-2)

CMS 25B COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT

The individuals whose signatures appear below, certify that they have destroyed the individual keytape segments on the dates indicated. Retain this form in accordance with Annex T.

CONFIDENTIAL (When filled in)

Seg	Signature	Signature	Date of Destruction
1A			
2A			
3A			
4A			
5A			
6A			
7A			
8A			
9A			
10A			
11A			
12A			
13A			
14A			
15A			
16A			
17A			
18A			
19A			
20A			
21A			
22A			
23A			
24A			
25A			
26A			
27A			
28A			
29A			
30A			
31A			

_____

(Command Title and Account Number)

_____	_____	_____	_____
SHORT TITLE	**EDITION**	**REG #**	**AL Code**

Classified by: CMS 1
Declassify on: Originating Agency's Determination Required.

CONFIDENTIAL (When filled in)

Figure 3-2A.—CMS 25B COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT (front).

CMS 25B COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT

The individuals whose signatures appear below, certify that they have destroyed the individual keytape segments on the dates indicated. Retain this form in accordance with Annex T.

CONFIDENTIAL (When filled in)

Seg	Signature	Signature	Date of Destruction
1A			
2A			
3A			
4A			
5A			
6A			
7A			
8A			
9A			
10A			
11A			
12A			
13A			
14A			
15A			
16A			
17A			
18A			
19A			
20A			
21A			
22A			
23A			
24A			
25A			
26A			
27A			
28A			
29A			
30A			
31A			

_____

(Command Title and Account Number)

SHORT TITLE	EDITION	REG #	AL CODE

Classified by: CMS 1

Declassify on: Originating Agency's Determination Required.

CONFIDENTIAL (When filled in)

Figure 3-2B.—CMS 25B COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT (back).

7. **CMS 25MC COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT—** The CMS 25MC is used to record destruction of multiple-copy segments of COMSEC keying material packaged in canisters (figure 3-3).

CMS Destruction

As a Radioman, you may very well be involved with the routine destruction of COMSEC material. The destruction methods that we discussed earlier are also used for COMSEC material. CMS 1 gives complete details on priority of destruction of CMS materials.

ROUTINE DESTRUCTION.— Superseded COMSEC material must be destroyed as soon as possible after supersession. Keying material marked "CRYPTO" must be destroyed no later than 12 hours after supersession. Superseded authentication publications and document; must be destroyed no later than 5 days after supersession.

EMERGENCY DESTRUCTION.— COMSEC material that must be destroyed in an emergency is divided into three categories:

- Keying material;
- COMSEC documents; and
- COMSEC equipment.

As we mentioned earlier, an emergency plan consists of both precautionary destruction and complete destruction.

PRECAUTIONARY DESTRUCTION.— When precautionary destruction is ordered, COMSEC material must be destroyed as follows:

CMS 25B COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT

The individuals whose signatures appear below, certify that they have destroyed the individual keytape segments on the dates indicated. Retain this form in accordance with Annex T.

CONFIDENTIAL (When filled in)

Seg/Copy #		Signature	Signature	Date of Destruction
1/01				
1/02				
1/03				
1/04				
1/05				
2/01				
2/02				
2/03				
2/04				
2/05				
3/01				
3/02				
3/03				
3/04				
3/05				

(Command Title and Account Number)

SHORT TITLE	EDITION	REG #	AL CODE

Classified by: CMS 1
Declassify on: Originating Agency's Determination Required.

CONFIDENTIAL (When filled in)

Figure 3-3.—CMS 25MC COMSEC KEYING MATERIAL LOCAL DESTRUCTION REPORT.

- **Keying Material—** Superseded keying material must be destroyed first, then keying material that becomes effective in 1 or 2 months.

- **Nonessential Classified COMSEC Documents—** This material includes maintenance, operating, and administrative manuals.

COMPLETE DESTRUCTION.— When complete destruction is ordered, COMSEC material must be destroyed as follows:

Keying Material— Keying material is always destroyed first in the following order: superseded, effective, then reserve.

Superseded keying material that has been used to encrypt traffic is the most sensitive of the three categories. If superseded keying material falls into enemy hands, all past intercepted traffic is subject to compromise and analysis. Superseded keying material must be destroyed within 12 hours after supersession.

Effective keying material is destroyed after superseded keying material. Reserve keying material is keying material that will become effective within the next 30 days. Reserve keying material is destroyed after effective keying material.

Keying material must be stored in priority order for destruction. Top Secret material must be destroyed ahead of Secret material, and Secret material destroyed ahead of Confidential material. This applies to all categories of keying material.

- **COMSEC Documents—** COMSEC documents are destroyed next. COMSEC documents include cryptoequipment maintenance manuals, operating instructions, general publications, status publications, CMS-holder lists and directories. COMSEC documents contain information on the types of cryptoequipments we use, the level of technology we have attained, and the way our COMSEC operations are organized and conducted.

- **COMSEC Equipment—** COMSEC equipment is destroyed last. In emergencies, the immediate goal regarding cryptoequipment is to render the equipment unusable and unrepairable. The operating and technical manuals for cryptoequipments provide details on the techniques for rapid and effective destruction.

VERIFY DESTRUCTION.— There are two parts to verifying the destruction of COMSEC material, witnessing and inspection of destroyed material.

Two individuals conducting the destruction must personally witness the complete destruction of the material. Then, they will sign and date the destruction documents after all material has actually been destroyed.

An inspection of the destroyed material must ensure that the destruction is complete and the destruction device is working properly. When using shredders, choppers, pulverizers or pulpers, you need only to examine a sample of the residue. If you are using an incinerator, verify that all residue is broken up by stirring or sifting through the remains.

The last detail is to inspect the surrounding area afterwards to ensure that no material escaped during the destruction process.

The destruction plan itself is contained in the overall emergency plan. The emergency plan should always provide for securing, removing, or destroying the material, depending on the situation.

The appropriate course of action and timing should be stated in the overall destruction plan. For example, if there is a local civil uprising that appears to be short-lived, destroying all material would probably not be necessary. In this situation, a partial destruction of the more sensitive superseded material might be made, some of the remaining material removed, and the rest secured.

The commanding officer will normally implement the emergency plan. Should the situation prevent contact with the commanding officer, other individuals, such as the COMSEC officer or COMSEC custodian, are usually authorized to implement the plan. During an emergency, personnel safety overrides the destruction priority.

TWO-PERSON INTEGRITY

Two-person integrity (TPI) is the security measure taken to prevent single-person access to COMSEC keying material and cryptographic maintenance manuals. TPI is accomplished as follows:

- The constant presence of two authorized persons when COMSEC material is being handled;

- The use of two combination locks on security containers used to store COMSEC material; and

- The use of two locking devices and a physical barrier for the equipment.

At no time can one person have in his or her possession the combinations or keys to gain lone access to a security container or cryptographic equipment containing COMSEC material. Neither can one person have sole possession of COMSEC material that requires TPI security.

CRYPTOGRAPHIC OPERATIONS AND OPERATOR REQUIREMENTS

As a Radioman, you will be required to learn and understand the more detailed procedures and processes involving cryptographic operations. Cryptographic procedures and associated equipments are governed by many strict rules and standards. To understand cryptographic operations and their importance, you must understand the following terminology:

CRYPTO— The marking "CRYPTO" is not a security classification. This marking is used on all keying material and associated equipment to protect or authenticate national security-related information. All material and equipment marked "CRYPTO" require special consideration with respect to access, storage, and handling.

CRYPTOMATERIAL— The term "cryptomaterial" refers to all material, such as documents, devices, or apparatus, that contain cryptoinformation. Furthermore, the material must be essential to the encryption, decryption, or authentication of telecommunications. Cryptomaterial is always classified and is normally marked "CRYPTO."

Cryptomaterial that supplies equipment settings and arrangements or that is used directly in the encryption and decryption process is called keying material. Keying material is afforded the highest protection and handling precautions of all information and material within a cryptosystem. Keying material is always given priority when an emergency plan is implemented.

CRYPTOINFORMATION— The category of cryptoinformation is always classified. This type of information normally concerns the encryption or decryption process of a cryptosystem. It is normally identified by the marking "CRYPTO" and is subject to all the special safeguards required by that marking.

- **CRYPTO-RELATED INFORMATION—** Crypto-related information may be classified or unclassified. It is normally associated with cryptomaterial but is not significantly descriptive of it. In other words, it does not describe a technique or process, a system, or equipment functions and capabilities. Crypto-related information is not marked "CRYPTO" and is not subject to the special safeguards normally associated with cryptoinformation.

- **CRYPTOSYSTEM—** The term "cryptosystem" encompasses all the associated items of cryptomaterial that are used together to provide a single means of encryption and decryption.

All items of a related nature that combine to form a system must be given the strictest security. Any failure, equipment, or operator that adversely affects the security of a cryptosystem is called cryptoinsecurity.

- **GENERAL AND SPECIFIC CRYPTOSYSTEMS—** During your cryptographic duties, you will sometimes hear the terms "general" and "specific" applied to some cryptosystems. A general cryptosystem consists of a basic principle and method of operation, regardless of the cryptomaterials used. In other words, regardless of the types of materials or elements used, the method of operation will always be the same, whether encrypting, decrypting, or authenticating.

A specific cryptosystem is one within a general system that is necessary and confined to actual encryption, decryption, or authentication. These systems are identified by the short and long titles of their variables.

- **CRYPTOVARIABLES—** A cryptovariable is an element of a cryptosystem that directly affects the encryption and decryption process. These variables are divided into two types: primary and secondary.

A primary cryptovariable is the most readily and frequently changed element of a cryptosystem. A secondary cryptovariable is one that permits change of circuit operation without altering the basic equipment. A secondary cryptovariable must also be used in conjunction with appropriate primary variables.

The commanding officer is responsible for ensuring that personnel are thoroughly trained and certified for cryptographic duties. This training may be formal or

on-the-job training. The CMS custodian is responsible for ensuring that cryptographic operators receive the training necessary to perform these duties and that they meet the following minimum qualifications:

- Be properly cleared for access to the material with which they will be working;
- Be authorized by the commanding officer to perform crypto duties; and
- Be familiar with local crypto procedures.

TRANSMISSION SECURITY

Transmission security results from measures designed to protect transmission from interception and exploitation by means other than cryptographic analysis. In the next paragraphs, we will discuss specific methods of transmission security.

COMMUNICATIONS SECURITY (COMSEC) EQUIPMENT

There are numerous types of cryptographic equipment used throughout the Navy. However, they all perform the same basic function—to encipher or decipher a communications signal.

During secure transmission, the cryptoequipment accepts a "plain text" teleprinter or data signal containing classified information from the classified (red) patch panel and adds a "key" (randomly chosen bits generated internally). This composite signal is relayed as an encrypted signal.

Following this encryption, the signal is fed to the unclassified (black) patch panel where it is patched directly to a converter. This converted audio signal is then routed to the transmitter for transmission.

Over-the-Air Rekey/Transfer (OTAR/OTAT)

Many of the new cryptosystems that use the 128-bit electronic key (ANDVT, KY-58, KG-84A/C, and KY-75) are now capable of obtaining new or updated key via the circuit they protect or other secure communications circuits. This process is known as *over-the-air rekey* (OTAR) or *over-the-air transfer* (OTAT). The use of OTAR or OTAT drastically reduces the distribution of physical keying material and the physical process of loading cryptoequipments with key tapes.

A station may have nothing to do with actual physical CRYPTO changeovers on a day-to-day basis. All an operator would have to do is observe the alarm indications and ensure the alarm indicator returns to operate. The electronic key would normally come from the Net Control Station (NCS).

The added feature of OTAT is that the key can be extracted from an OTAT-capable cryptosystem using a KYK-13 or KYX-15/KYX-15A. The key is then loaded into another cyptosystem as needed. More detailed information on OTAR/OTAT is available in the *Procedures Manual for Over-the-Air Transfer (OTAT) and Over-the-Air Rekey (OTAR)* and *Field Generation and Over-the-Air Distribution of Tactical Electronic Key, NAG-16C/TSEC.*

Authentication

Authentication is a security measure designed to protect a communications or command system against fraudulent transmissions or simulation. Authenticating systems have instructions specifying the method of use and transmission procedures. By using an authenticating system properly, an operator can distinguish between genuine and fraudulent stations or transmissions. A station may include authentication in a transmitted message. This security measure is called transmission authentication. The types of authentication are:

- **Challenge and Reply—** This is a prearranged system whereby one station requests authentication of another station (the challenge). By a proper response, the latter station establishes its authenticity (the reply).
- **Transmission Authentication—** A station establishes the authenticity of its own transmission by either a message- or a self-authentication method. A message authentication is a procedure that a station uses to include an authenticator in the transmitted message. Self-authentication is a procedure that a station uses to establish its own authenticity, and the called station is not required to challenge the calling station.

The following examples are instances when authentication is mandatory:

- A station suspects intrusion on a circuit;
- A station is challenged or requested to authenticate;
- A station directs radio silence or requires another station to break an imposed radio silence; and

- A station transmits operating instructions that affect communications, such as closing down a station, shifting frequency, or establishing a special circuit.

You can find further information on authentication in *Communications Instructions—Security (U),* ACP 122.

MEACONING, INTRUSION, JAMMING, AND INTERFERENCE (MIJI)

MIJI is a term used to describe four types of interference that you are likely to experience in a given situation.

Meaconing is the interception and rebroadcast of navigation signals. These signals are rebroadcast on the received frequency to confuse enemy navigation. Consequently, aircraft or ground stations are given inaccurate bearings. Meaconing is more of a concern to personnel in navigation ratings than to you as a Radioman. However, communications transmitters are often used to transmit navigation signals. Since communications personnel operate the transmitters, they must know how to deal with any communications problems resulting from meaconing.

Intrusion is defined as any attempt by an enemy to enter U.S. or allied communications systems and simulate our traffic to confuse and deceive. An example of intrusion is an unauthorized radio transmission by an unfriendly source pretending to be part of an air traffic control service and giving false instructions to a pilot.

Jamming is the deliberate radiation, reradiation, or reflection of electromagnetic signals to disrupt enemy use of electronic devices, equipment, or systems. In jamming operations, the signals produced are intended to obliterate or obscure the signals that an enemy is attempting to receive. Some common forms of jamming include:

- Several carriers adjusted to the victim frequency;
- Random noise amplitude-modulated carriers;
- Simulated traffic handling on the victim frequency;
- Random noise frequency-modulated carriers;
- Continuous-wave carrier (keyed or steady); and
- Several audio tones used in rapid sequence to amplitude modulate a carrier (called bagpipe from its characteristic sound).

Interference is normally a nondeliberate intrusion upon a circuit. It unintentionally degrades, disrupts, obstructs, or limits the effective performance of electronic or electrical equipment. Interference usually results from spurious emissions and responses or from intermodulation products. Sometimes, however, interference may be induced intentionally, as in some forms of electronic warfare. An example of interference is the interruption of military transmissions by a civilian radio broadcast.

The more effective methods of dealing with MIJI are contained in *Fleet Communications,* NTP 4, and in *Reporting Meaconing, Intrusion, Jamming, and Inteference of Electromagnetic Systems,* OPNAVINST 3430.18.

SUMMARY

In this chapter we introduced you to the basic concepts of communications security, described various cryptosystems, and familiarized you with the procedures and methods of transmission security.

As a Radioman, you have a two-fold job concerning security. The first, of course, is to properly perform your duties within general security guidelines. Security guidelines pertain to everyone in every official capacity. Second, you must also perform your duties in such a manner as to protect the integrity and overall value of secure communications.

Security violations result from bad personal habits, security indifference, occupational fatigue, or ignorance of established regulations. When security violations occur in installations located in foreign countries, the violations become more serious because of an activity's greater vulnerability to hostile exploitation. With respect to COMSEC, security violations could prove costly.

Security precautions mentioned in this chapter do not guarantee complete protection, nor do they attempt to meet every conceivable situation. Anyone who adopts a commonsense outlook can, however, solve most security problems and gain a knowledge of basic security regulations. For information on local security rules, study your command's security regulations.

CHAPTER 4

AIS SECURITY

LEARNING OBJECTIVES

Upon completing this chapter, you should be able to do the following:

- *Identify the procedures for issuing and updating user identification and passwords and for validating customer authorization.*
- *Identify the procedures for performing, directing, and validating security inspections and for reporting and investigating security violations.*
- *Identify the procedures for developing and updating security plans.*
- *Recognize how to implement and evaluate countermeasures and contingency plans.*
- *Identify the procedures for preparing and updating emergency action plans.*
- *Ekplain how to implement and evaluate security test and evaluation procedures.*
- *Explain how to safeguard AIS classified material.*

AIS security is a cycle of events that never ends. You start with the development of a security plan for the facility. This plan includes conducting an in-depth risk assessment covering different types of disasters that threaten the security of the AIS facility. Once the security plan is in place, the inspections begin. You will be responsible for preparing the inspection plan and conducting the inspection using the guidelines provided in the security instructions.

In this chapter, you will learn about AIS security—from the implementation of the security plan through conducting security inspections. This includes AIS threat and risk analysis, disaster protection, contingency planning, inspection preparation, and data privacy.

WHAT IS AIS SECURITY?

AIS security is more than protecting classified information and keeping unauthorized personnel out of your AIS facility. It is protecting equipment, media, data and people. AIS security is limiting access, avoiding misuse, and preventing destruction. It is preventing changes to data that would make the data unreliable. It covers the denial of service and the destruction of computer rooms, the loss of confidentiality, fraud, the theft of computer time as well as the computer itself. AIS security is a critical part of your job.

As you probably noticed from reading the learning objectives, AIS security has its own terminology and jargon. To carry out your AIS responsibilities, you need to be familiar with these terms and their meanings.

AIS SECURITY CONCEPTS

Our AIS security goal is to take all reasonable measures to protect our AIS assets. Keep in mind that AIS assets (hardware, software, data, supplies, documentation, people, and procedures) have value.

Their value can usually be stated in dollar terms. It costs money to repair or replace hardware. It costs money to reprogram and redocument. It costs money to retrain personnel. Unauthorized access costs money. Service delays cost money.

AIS Assets

Our AIS assets (figure 4-1) include the facilities, hardware, software, data, supplies, documentation, people and procedures. These assets combine to provide service. Service is computer time, telecommunications, data storage, user support, application system development, and operation. Service must be available to those authorized to receive it when they request it. Information is at the top of the triangle. It is the ultimate AIS asset. Information is the reason the rest exists.

Threats

Threats are things that can destroy your assets (figure 4-2). Easy to recognize, threats come in two basic forms: people and environmental changes. People are a threat because they sometimes do unexpected things, make mistakes, or misuse resources, steal, subvert, and sabotage (deliberate threats). Some of us even smoke and spill soft drinks in computer rooms. Environmental threats are things like heat, humidity, explosions, dust, dirt, power peaks, power failures; and natural disasters like fire, floods, hurricanes, thunderstorms, and earthquakes. Hardware failures and compromising emanations are also threats. Another term associated with threats is their probability of occurrence. What is the likelihood that something will happen? Probabilities are measured in time—once a pico second, once a memory cycle, once a fiscal year, once a century.

Vulnerability

Threats cannot reach an AIS asset without the aid and assistance of a vulnerability. Vulnerabilities are the holes threats sneak through or weaknesses they exploit. Vulnerabilities are caused by lack of AIS security planning, poor management, disorganization, disorder, inadequate or improper procedures, open data and open door policies, undocumented software, unaware or unconcerned personnel. You can help limit the vulnerabilities by following established AIS security. policies and procedures.

Successful Attacks and Adverse Events

Successful attacks and adverse events result from a combination of threats, vulnerabilities, and AIS assets. When a threat takes advantage of a vulnerability and does harm to your AIS assets, a successful attack or adverse event has occurred. Successful attacks and adverse events may be roughly grouped as losses or abuses. You can lose hardware, software, and data. You can lose documentation and supplies. You can lose key staff personnel. Losses often result in denial of service, preventing access to information when it is

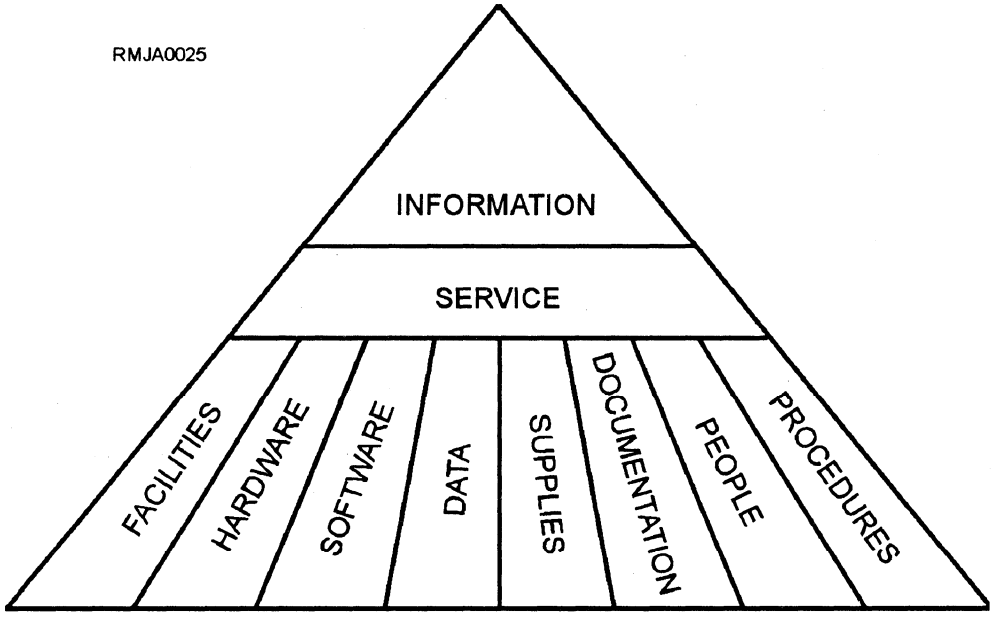


Figure 4-1.—AIS assets.

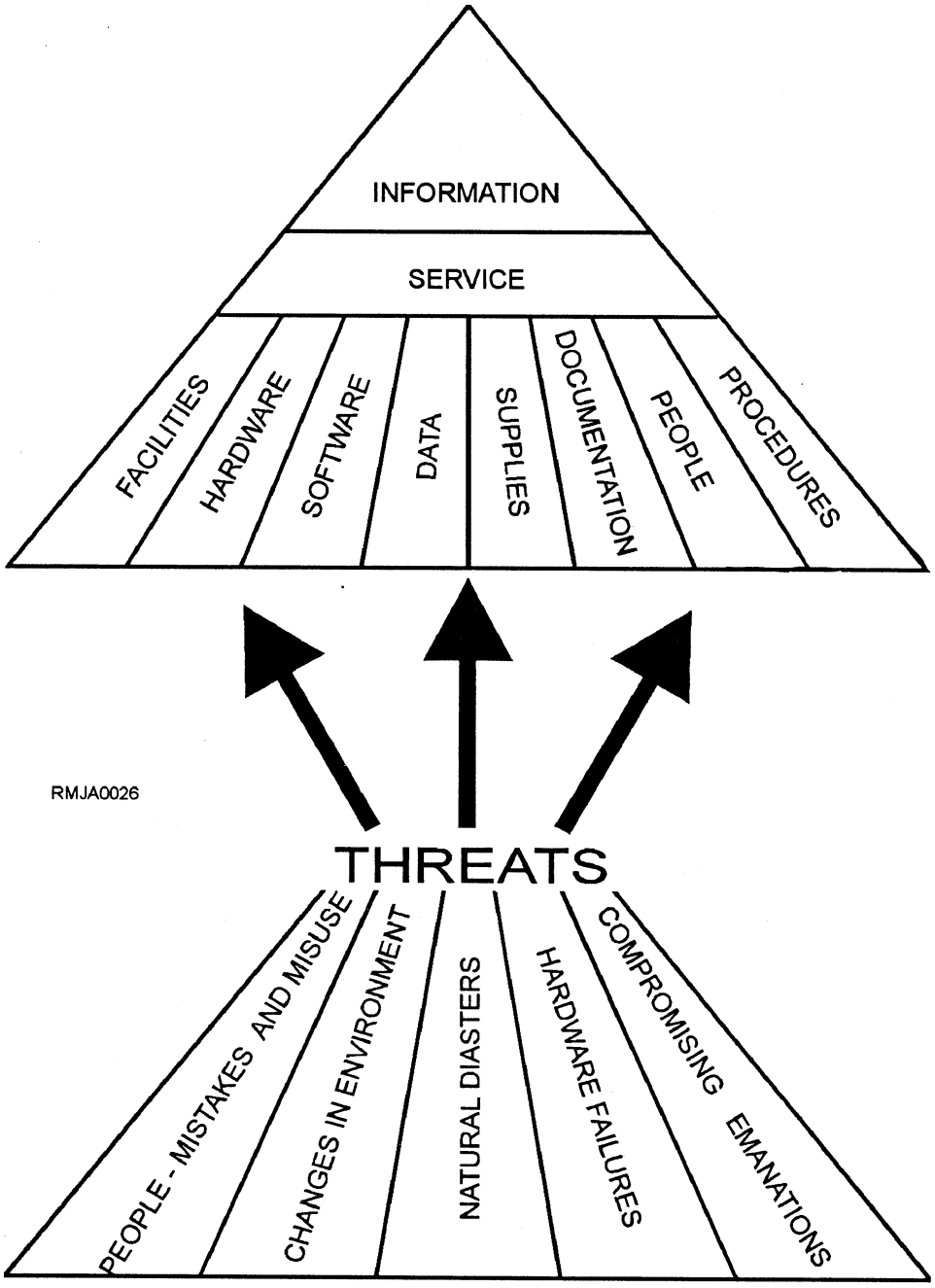


Figure 4-2.—Threats to AIS assets.

needed. Abuse relates to unauthorized access to service, unwanted destruction or alteration of data and software, and unauthorized disclosure of classified information.

We have an adverse event with every fire and with every flood caused by a broken pipe in a computer room. We have a successful attack with every bowling score, recipe, or school paper stored online, and with every computer hacker that plays crash-the-computer or scramble-the-data.

Likelihood and Risk

Likelihood and risk relate to successful attacks and adverse events. Likelihood relates to chance-what is the likelihood (probability) that a successful attack or an adverse event will occur? Risk has to do with money; it tells us about the cost of loss or abuse from an adverse event overtime. We first ask, "What is the value of the AIS asset that will be abused or that we will lose if a given successful attack or adverse event occurs?" Then we ask, "How often can we expect that

particular attack or event to occur?" Remember, the successful attack or adverse event results from a particular threat exploiting a particular vulnerability. It is very specific reasoning. The greater the value of the AIS asset and the more likely the successfid attack or adverse event, the greater the risk. Figure 4-3 shows this risk analysis concept. Risks are usually expressed in terms of dollars per year, the annual loss expectancy.

Countermeasures

Once the threats and vulnerabilities are known and the likelihood and risk of a successful attack or an adverse event are determined, a plan is developed to set up countermeasures (controls) to lessen or eliminate the vulnerabilities. If you have a countermeasure, you have a protected vulnerability. If you have an unprotected vulnerability, you do not have a countermeasure. Some countermeasures help us prevent adverse events, whereas others detect adverse events. We have measures to minimize the effects of successful attacks or adverse events. We also have measures, called contingency plans, to recover from a successful attack or an adverse event. Figure 4-4 gives an example of each type of security measure strategy as it relates to fire loss. Figure 4-5 shows threats, vulnerabilities, and countermeasures to our assets.

Another way to categorize countermeasures is by type: physical, technical, administrative, and managerial (figure 4-6).

PHYSICAL CONTROLS.— We usually think of physical control first. They include the locked computer room door, physical layout, fire extinguishers, access barriers, air conditioners, moisture detectors, and alarms.

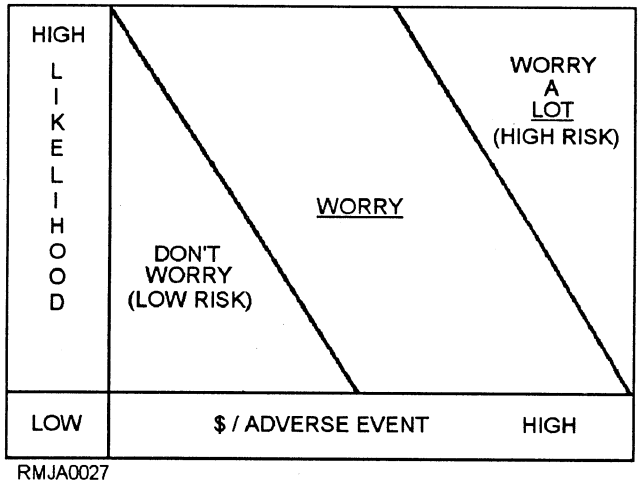


Figure 4-3.—MS security risk analysis.

TECHNICAL CONTROLS.— Technical controls are embedded in hardware, software, and telecommunications equipment. They are diagnostic circuitry, component redundancies, and memory protect features. They are controls built into the operating system. They include log-on IDs and passwords to enable only authorized users access to the computer system. They are accounting routines, encryption coding, and audit trails.

ADMINISTRATIVE CONTROLS.— Administrative controls concern people and procedures. They include who is authorized to do what, methods to keep track of who enters a sensitive area, who receives a delivery, and who requests a sensitive report. The operating procedures you follow will sometimes include security requirements. You are responsible for adhering to the procedures to ensure AIS requirements are met.

MANAGERIAL CONTROLS.— Managerial controls tie everything together. They concern planning and evaluation. They include audits to review the effectiveness and efficiency of the countermeasures. They check to make sure that the measures are actually in place, being followed, and working. Problems found require replanning and reevaluation to see that corrections are made.

RISK MANAGEMENT

Risk management involves assessing the risks, determining loss potential estimates, and selecting countermeasures appropriate to prevent, detect, minimize, and recover from successful attacks and adverse events. Management selects the countermeasures, making sure that the cost of the measure is less than the cost of the risk. The trick is to select the countermeasure that will result in the lowest total cost while taking all reasonable measures to protect our AIS assets.

Keep in mind that the presence of a vulnerability does not in itself cause harm. A vulnerability is merely a condition or set of conditions that may allow the computer system or AIS activity to be harmed by an attack or event. Also, keep in mind that an attack made does not necessarily mean it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures. Countermeasures may be any action, device, procedure, technique, or other measure that reduces the vulnerability of an AIS activity or computer system to the realization of a threat.

COUNTERMEASURE STRATEGY FOR FIRE LOSS			
PREVENT	DETECT	MINIMIZE	RECOVER
CLEAN ROOM SECURE CABLES AND CONNECTIONS NO SMOKING	SMOKE DETECTOR	HALON OFF-SITE DATA STORAGE	CONTINGENCY PLAN ALTERNATE COMPUTER USE

RMJA0028

Figure 4-4.—An example of countermeasures against fire loss.

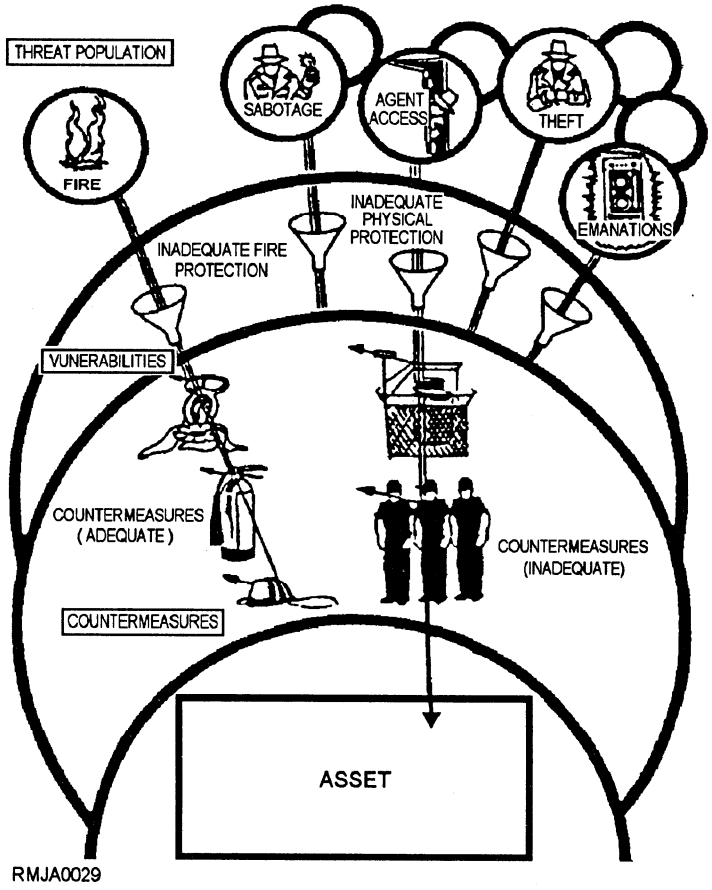


Figure 4-5.—Threats, vulnerabilities, and countermeasures.

Not all attacks and events can be avoided. If we cannot reasonably prevent something, we want to detect the problem as early as possible, minimize the damage and destruction, and recover as quickly and efficiently as possible. To help us minimize and recover, we develop contingency plans.

Contingency plans (backup plans) provide for the continuation of an activity's mission during abnormal operating conditions. These are plans for emergency response, backup operations, and post-disaster recovery. They include a preparation phase that includes the steps to be taken in anticipation of a loss to

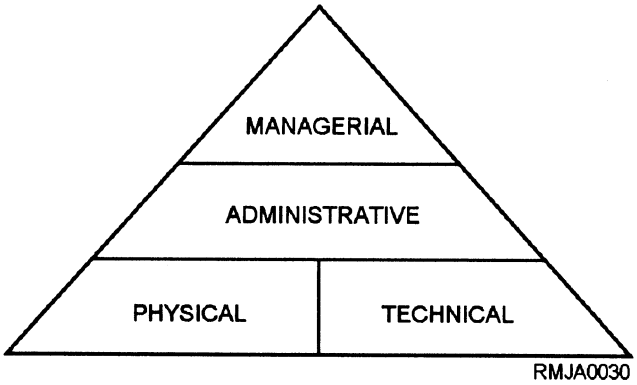


Figure 4-6.—Types of AIS security countermeasures.

lessen damage or assist recovery. The action phase includes the steps to be taken after a successful attack or adverse event to minimize the cost and disruption to the AIS environment.

SCOPE OF AIS SECURITY

As the Navy has become increasingly dependent on the use of AIS for its payroll, supply functions, tactical information, and communications, the need to protect AIS assets has taken on greater importance. Risk management is an ongoing effort. Whether you are in a large AIS facility with a full-time information system security manager (ISSM) or a facility where the functions of the ISSM are a collateral duty, your installation will have established security measures to protect its AIS assets.

The five areas of consideration for the Navy's AIS security program are hardware (I), data (II), human resources (III), software (IV), and communications (COMM) (V). These are shown in figure 4-7. Because each AIS facility is different, each facility has its own AIS security risk management program. You'll be responsible for following the requirements of your facility's AIS security program.

In the next paragraphs, you will learn about management responsibilities, your responsibilities, physical security measures, and data security measures. Again, our goal in AIS security is to prevent or minimize the opportunity for modification, destruction, disclosure, or denial of service.

MANAGEMENT RESPONSIBILITY

AIS security is everyone's responsibility, and only the commanding officer (CO) can ensure that AIS security receives the support required at every level. The success of your command's AIS security program depends upon the support of the CO. The CO and the AIS security staff are responsible for taking the necessary steps to provide an adequate level of security for all AIS-related activities, automated information systems, and networks, including those developed, operated, maintained, or provided by contractors.

Each AIS facility has an information system security manager (ISSM). His or her primary duty is to serve as the single point of contact for all matters relating to AIS security at your command. The ISSM usually reports directly to the CO. Now, let's talk a little about the security staff.

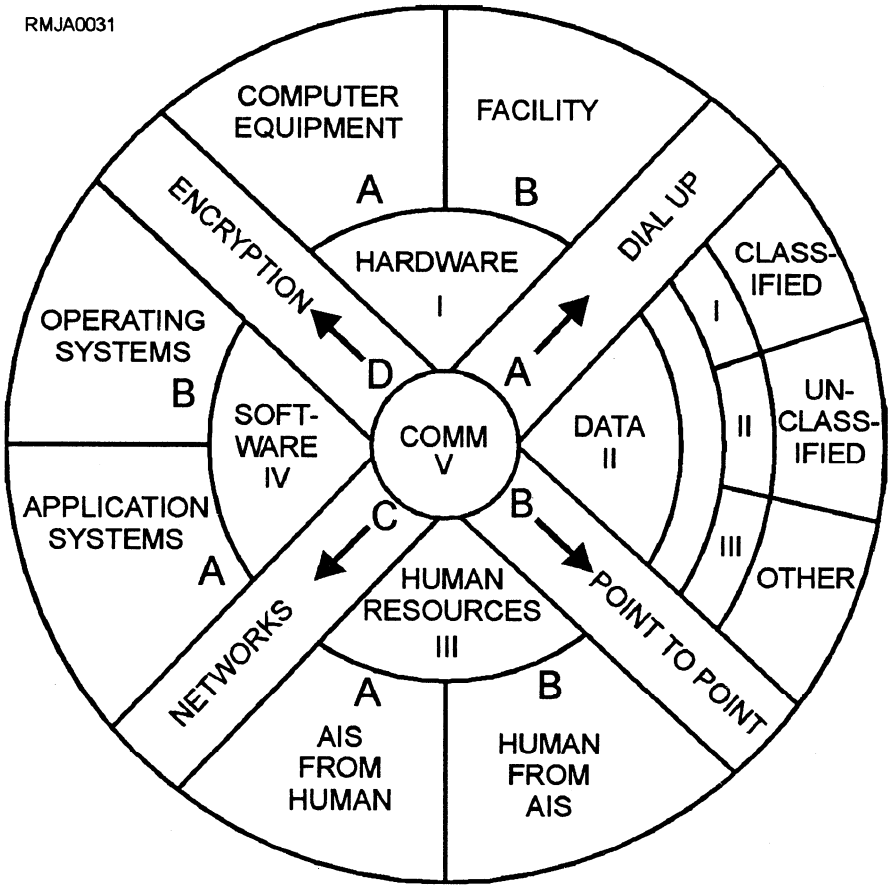


Figure 4-7.—Department of the Navy AIS security areas.

Many factors determine the numbers and types of people assigned to the AIS security staff. These factors include the type of activity, its size, its hardware configuration(s), types of work to be processed, and so on. Your command's AIS security staff may include any one, several, or all of the following people:

- Command security manager;
- Information system security manager (ISSM);
- Information system security officer (ISSO);
- Network security officer (NSO);
- Terminal area security officer (TASO).

These people are specialists. Some day you may be one of them. They have been trained and are knowledgeable in such areas as the following:

- General security awareness;
- User and customer security;
- Security administration;
- Security violation reporting;
- Hardware and software security;
- Systems design security;
- Terminal and device related security;
- Telecommunications security;
- Physical security;
- Personnel security;
- Computer auditing;
- Data security;
- Risk assessment methodology;
- Contingency and backup planning;
- AIS security and Navy contractors;
- Disaster recovery;
- Security accreditation; and
- Security test and evaluation.

From this list you can see that AIS security is a complex area and requires many specialized skills and knowledges. In addition, each member of the AIS security staff is responsible for ensuring that you are adequately trained in AIS security. Do you know the name of your command ISSM? If not, seek him or her out and find out what your responsibilities are, rather than finding out the hard way through a bad experience. That brings us to your responsibilities.

PERSONAL RESPONSIBILITY

You play an important role in the success of your command's security program. As we stated earlier, security is everybody's job, from seaman recruit to admiral.

Do not leave listings unattended or files open for unauthorized browsing. If you see a stranger in your work area, it is your job to confront (challenge) that individual regardless of his or her rate or rank, job title, or status within or outside of your command. For the most part, you know who is authorized to be in your work area.

As a computer operator, you are responsible for protecting hardware from fire, flood, sabotage, and internal tampering. You are also concerned with protecting applications software, systems software, program and data files, and all forms of input and output media with which you will be working.

If you are working in the magnetic media library, you are responsible for protecting all library-related equipment (tape/disk cleaners, tape degaussers, tape/disk certifiers, and so on). If you are handling and working with classified media and materials, you must handle, store, and dispose of them in accordance with established procedures. The same rules apply regardless of what area you maybe working in; whether you are a data entry operator, a control clerk in production control (I/O), a computer programmer, or an analyst. All positions require you to pay attention to AIS security. The key word is *protect.*

Believe it or not, AIS security is not really that difficult to understand, nor is it difficult to carry out. Sixty-five percent of it is nothing more than using good old common sense; the remaining thirty-five percent comes from awareness that you get through proper training.

Try thinking of AIS security and protecting its related assets the same way you would protect your home and personal effects. In AIS we are talking millions of dollars, some of them yours. Think about the kind of AIS security you would want to have installed if that AIS facility were yours and what you would do to protect all its assets.

From this point on, the rest is up to you. Stay alert, keep your eyes and ears open to what is going on around

you, and never hesitate to challenge or question someone or something that you feel is wrong or out of character.

PHYSICAL SECURITY MEASURES

Physical security is the one area with which you are most likely to be familiar. It deals with such things as personnel, the environment, the facility and its power supply(ies), fire protection, physical access, and even the protection of software, hardware, and data files.

Your command must provide physical security for your AIS facility. The degree of physical security at your installation or command depends on its physical characteristics, its vulnerability within the AIS environment, and the type of data processed. Minimum physical security requirements include four basic areas that your command must address: physical security protection, physical access controls, data file protection, and natural disaster protection.

- **Physical security protection.** Physical security protection takes on two forms. The first is physical barriers, such as solid walls, caged-in areas, bulletproof glass, locked doors, and even continual surveillance of the controlled area. The second involves people and the procedures that you must follow, such as looking up names on the access list to determine who is authorized in a given space or area. There are also escort procedures you must follow to be sure that your party gets to the right place and/or person.
- **Physical access controls.** Physical access controls are implemented to prevent unauthorized entry to your computer facility or remote terminal areas. Physical access controls can be accomplished in several ways: conventional key and lock set, electronic key system, mechanical combination lock, or electronic combination lock. Regardless of the type of system installed at your command, it is important to remember that keys belong on your key-ring or chain, electronic keys or cards should be in your possession at all times (except when sleeping), and combinations should be memorized, not written down somewhere for everyone to see.
- **Data file protection.** Physical access to data files and media libraries (magnetic disks, tape files, microforms, and so on) is authorized only to those personnel requiring access to perform their job.
- **Natural disaster protection.** The effects of natural disasters must be prevented, controlled, and minimized to the extent economically feasible by the use of detection equipment (heat sensors, smoke detectors), extinguishing systems, and well conceived and tested contingency plans.

Environmental Security

Temperature and humidity can affect the operation of your computer facility. Whenever possible, computer equipment is operated within the manufacturer's optimum temperature and humidity range specification. Fluctuations in temperature and/or humidity over an extended period of time can cause serious damage to the equipment. So, with that in mind, you are probably asking yourself, "What are the acceptable levels for computer operation?" Normally, you can find this information in the command's standard operating procedures (SOPs), or you can check with your supervisor. If neither are available, a safe rule of thumb is a temperature of 72° Fahrenheit, ±2°, and a humidity of 55%, ±5%.

To maintain a constant temperature and humidity to the computer facility or remote terminal areas, keep all doors and windows closed. Because temperature and humidity are vitally important to computer performance, it is essential that only designated personnel be allowed to regulate these types of environmental controls.

If your workspace has a recording instrument to monitor the temperature and humidity, by all means check it periodically to be sure it is within the prescribed limits. If you notice a significant fluctuation (up or down), notify your supervisor.

Some devices have built-in warning signals (a light, audible sound, or both) to warn you of near-limit conditions for temperature and/or humidity.

Lighting

You are responsible for ensuring that adequate lighting is maintained. Be particularly attentive to emergency lights. If they are not functioning properly, report the problem to your supervisor as soon as possible. Emergency lights are installed for your protection and safety, not for the safety of the equipment. They are there to ensure a quick exit if you must evacuate in a hurry.

Physical Structure Security

In the Navy we often decide we need computer equipment and then wonder where we are going to install it. The existing building (or shipboard compartment) may not lend itself to the physical security requirements needed to protect the system.

Things like false overheads (ceilings) can conceal water and steam pipes. The pipes should be checked on a regular basis and any irregularities reported immediately. Personnel should be familiar with the locations and operation of the cut-off valves for the pipes. Air-conditioning ducts in the overhead, if not properly insulated, can result in condensation, causing water to drip down on the computer.

When repair work is scheduled within the computer spaces (working under the raised floor or in the overhead), be sure to take all necessary precautions to protect the equipment. Use plastic sheeting to cover the system (particularly the CPU). Watch out for overhead water or steam pipe bursts and for activated sprinkler systems. Ensure maximum personnel safety, while keeping disruption to a minimum. Dust coming from the work area can damage the equipment: clogged filters result in overheated components, a head crash on a disk drive, dirty read/write heads on tape drives, and so on. Remember, the key word is to protect all AIS assets.

WARNING

Should your equipment be exposed to water, do not turn it on until it has been thoroughly checked out by qualified maintenance personnel.

Power Supply Protection

Your computer facility and remote terminal areas require adequate power. Variations in electrical power can affect the operation of computer equipment. Most computer equipment is designed in such away that it is able to rectify the incoming ac current, filter it, and regulate the resulting dc current before it is applied to the computer circuitry. However, this filtering and regulation cannot be expected to eliminate voltage variations beyond a reasonable range. Power fluctuations can cause unpredictable results on hardware, logic, and data transfer. Should your system encounter such fluctuations, it is highly recommended that the equipment be shut down at once until the problem is corrected.

Some computer systems are equipped with an uninterrupted power source (UPS). A UPS provides the auxiliary power for your equipment that may be required if your command's mission dictates continuous AIS support to fulfill its obligations or if your computer system is in an area where there are frequent brownouts. Auxiliary power should be checked on a periodic basis.

Fire Protection

Fire protection is one of the major elements of any command's physical security program. All personnel (military and civilian) receive periodic training in emergency procedures in case of fire. The training usually includes, at a minimum, proper equipment shutdown and startup procedures, information about your fire detection and alarm systems, use of emergency power (especially aboard ship), use of fire-fighting equipment, and evacuation procedures.

Master control switches are used to shut off all power to your AIS spaces in the event of fire. If your air-conditioning system is not setup for smoke removal, it is probably connected to the master control switches. The master control switches are normally located at the exit doors, so in an actual emergency you do not have to pass through a dangerous area to activate the switches. These switches should be easily recognizable. They are clearly labeled and protected to prevent accidental shutdown. Commands that process critical applications will have master control switches that allow for a sequential shutdown procedure of your equipment. Learn the location of the switches and procedures used in your computer spaces.

There will be enough portable fire extinguishers for you to fight a relatively small or self-contained fire. Extinguishers are placed within 50 feet of the computer equipment. Prominently displayed markings and/or signs are above each extinguisher, and each is easily accessible for use.

WARNING

Be sure to use only carbon dioxide or inert-gas fire extinguishers on electrical fires.

One final note. Experience has shown repeatedly that prompt detection is a major factor in limiting the amount of fire damage. Computer areas require a fire detection system capable of early warning and with an automatic fire extinguishing system.

Hardware Protection

Hardware security is defined in the *Department of the Navy Automatic Data Processing Security Program,* OPNAVINST 5239.1, as "Computer equipment features or devices used in an AIS system to preclude unauthorized, accidental or intentional modification, disclosure, or destruction of AIS resources."

DATA PROTECTION MEASURES

FIPS (Federal Information Processing Standards) PUB 39 *Glossary for Computer Systems Security* defines data security as "The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure." We are always concerned with the integrity of data; is the data the same as that in the source documents? We want to ensure that the data has not been exposed to accidental or intentional modification, disclosure, or destruction.

Depending on the type of data being processed, the other users with access to the system, and the technical features of the system to provide the needed safeguards, the system may have to operate in a specific security mode.

If your command processes classified and/or sensitive unclassified data, it must abide by certain rules to protect it. In the central computer facility (where the host computer is located), the physical security requirements will be equal to the highest classification of data being handled. If there are two or more computer systems located in the same controlled area, the systems should be separated to limit direct personnel access to a specific system.

In remote terminal areas, security requirements are based upon the highest classification of data to be accessed through the terminals. Each remote terminal must be identifiable through hardware or software features when it is connected to a computer system or network processing classified data. The system or network must know who is logging on.

If the computer system to which your remote terminal is connected is processing classified data and your terminal is not authorized, controlled, or protected for that classification of data, it must be disconnected. The disconnect procedures may be by a hardware measure (such as turning off a switch at the host computer) or a software measure (such as deleting the ID of your terminal during certain processing periods). Because each data classification has different security requirements, we cover each separately.

Classified Data

Handling requirements and procedures for classified AIS media (Confidential, Secret, and Top Secret) are the same as those for handling classified information. Anyone who has possession of classified material is responsible for safeguarding it at all times. You need to be familiar with the four security modes that provide for processing classified data: system high, dedicated, multilevel, and controlled.

SYSTEM HIGH SECURITY MODE.— A computer system is in the system high security mode when the central computer facility and all of the connected peripheral devices and remote terminals are protected in accordance with the requirements for the highest classification category and type of material then contained in the system. All personnel having computer system access must have a security clearance, but not necessarily a need-to-know for all material then contained in the system. In this mode, the design and operation of the computer system must provide for the control of concurrently available classified material in the system on the basis of need-to-know.

DEDICATED SECURITY MODE.— A computer system is operating in the dedicated security mode when the central computer facility and all of its connected peripheral devices and remote terminals are exclusively used and controlled by specific users or group of users having a security clearance and need-to-know for the processing of a particular category(ies) and type(s) of classified material.

MULTILEVEL SECURITY MODE.— A computer system is operating in the multilevel security mode when it provides a capability permitting various categories and types of classified materials to be stored and processed concurrently in a computer system and permitting selective access to such material concurrently by uncleared users and users having differing security clearances and need-to-know. Separation of personnel and material on the basis of security clearance and need-to-know is accordingly accomplished by the operating system and associated system software. In a remotely accessed resource-sharing system, the material can be selectively accessed and manipulated from variously controlled terminals by personnel having different security clearances and need-to-know. This mode of operation can accommodate the concurrent processing and storage of (1) two or more categories of classified data, or (2) one or more categories of classified data with unclassified data, depending upon the constraints

placed on the system by the designated approving authority.

CONTROLLED SECURITY MODE.— A computer system is operating in the controlled security mode when at least some personnel (users) with access to the system have neither a security clearance nor a need-to-know for all classified material then contained in the computer system. However, the separation and control of users and classified material on the basis, respectively, of security clearance and security classification are not essentially under operating system control as in the multilevel security mode.

Sensitive Unclassified Data

Sensitive unclassified data is unclassified data that requires special protection. Examples are data For Official Use Only and data covered by the Privacy Act of 1974.

The Privacy Act of 1974 imposes numerous requirements upon federal agencies to prevent the misuse of data about individuals, respect its confidentiality, and preserve its integrity. We can meet these requirements by applying selected managerial, administrative, and technical procedures which, in combination, achieve the objectives of the Act.

The major provisions of the Privacy Act that most directly involve computer security are as follows:

- Limiting disclosure of personal information to authorized persons and agencies;
- Requiring accuracy, relevance, timeliness, and completeness of records; and
- Requiring the use of safeguards to ensure the confidentiality and security of records.

To assure protection for AIS processing of sensitive unclassified data, the Navy has established the limited AIS access security mode.

A computer system or network is operating in the limited access security mode when the type of data being processed is categorized as unclassified and requires the implementation of special access controls to restrict the access to the data only to individuals who by their job function have a need to access the data.

Unclassified Data

Although unclassified data does not require the safeguards of classified and sensitive unclassified data, it does have value. Therefore, it requires proper handling to assure that it is not intentionally or unintentionally lost or destroyed.

AIS MEDIA PROTECTION MEASURES

AIS media protection is important because that is where we store data, information, and programs. All data and information, whether classified or not, require some degree of protection. Software also requires protection. You would not want to lose the only copy of a program you had worked 4 months to write, test, and debug. The amount of protection depends on the classification of data, the type of AIS storage media used, the value of the material on it, and the ease with which the material can be replaced or regenerated. AIS media includes magnetic tapes, disks, diskettes, disk packs, drums, cathode-ray tube (CRT) displays, hard copy (paper), core storage, mass memory storage, printer ribbons, carbon paper, and computer output microfilm and microfiche.

You are responsible for controlling and safeguarding (protecting) the AIS media at all times. For purposes of control, AIS media can be divided into two types or categories: working copy media and finished media. You will be working with both.

Working copy media is temporary in nature. It is retained for 180 days or less and stays within the confines and control of your activity. Examples of working copy media are tapes and disk packs that are used and updated at frequent intervals and coding forms that are returned immediately to the user after processing.

Finished media is permanent in nature. It includes tapes and disk packs, hard-copy output, or any other AIS media containing data or information to be retained for more than 180 days. Finished media can be released to another activity. For example, a magnetic tape can be sent to another activity as a finished media. However, the receiving activity may treat it as working copy media if it is kept 180 days or less. Of course, AIS media, whether working copy or finished copy, requires the use of security controls.

Security Controls

The security controls we discuss are general in nature and are considered the minimum essential controls for protecting AIS media. Your activity's standard operating procedures (SOPS) are designed to ensure that an adequate level of protection is provided. Classified working copy media must be dated when created, marked, and protected in accordance with the

highest classification of any data ever recorded on the media. If classified working copy media is given to a user, the user is then responsible for its protection.

Classified finished media must be marked and accounted for. You may be responsible for inventorying magnetic tapes, disk packs, and other forms of AIS media. Your activity must maintain a master list of AIS media that is classified as Secret or Top Secret. This master list includes the overall security classification of the media and the identification number permanently assigned to it. The media must also be controlled in the same manner prescribed for classified material outside an AIS environment. For additional information, consult the *Department of the Navy Information and Personnel Security Program Regulation*, OPNAVINST 5510.1 (hereinafter called the *Security Manual).*

Security Markings

Your activity will have procedures for marking AIS media. These are important to protect the media from unauthorized, accidental, or intentional disclosure, modification, destruction, or loss. You can imagine how easy it is to pickup an unmarked tape, load it on the tape drive, and have whatever is on it recorded over by a program. You have probably done this to tapes with your tape cassette recorder/player. This is why we have mechanical means, like tape rings and diskette notches, to protect magnetic media. These methods, combined with clearly marked labels, go a long way toward protecting data and programs on magnetic media. Let's look at the types of markings the Navy uses for the various types of media for marking classified data.

MAGNETIC MEDIA.— Each magnetic tape, diskette, and disk pack must be externally marked with a stick-on label with the overall security classification and a permanently assigned identification number. When the tapes, diskettes, and disk packs are to be declassified by degaussing, all external labels indicating the classification must be removed unless the media will be immediately used to store information of the same classification. Many installations set aside groups of tapes and disks for recording classified data at each security level.

HARD-COPY REPORTS, MICROFILM, AND MICROFICHE.— Hard-copy reports or printouts from a printer, terminal, plotter, or other computer equipment and microfilm and microfiche must be properly marked. Those prepared during classified processing must be marked at the top and bottom of each page with the appropriate classification or the word "unclassified," and each page should be consecutively numbered.

CRT DISPLAYS.— The appropriate security classification marking is displayed at the top of the screen when displaying classified data or information.

Disposition of Media

There comes a time when the media or the information on the media is no longer needed. With microfilm, microfiche, and printouts, we destroy the media with the data. The same is not true of magnetic media. We can erase and reuse the media when the data is no longer needed. However, the media cannot function forever. Tapes and disks become damaged or eventually wear out.

When a disk or tape becomes unusable, it must be disposed of. But first, each disk and tape must be accounted for. It may have been used for classified data. The magnetic media librarian will see that it is disposed of properly. If the media contained classified data, it will be degaussed before being destroyed.

There are two other problem areas we tend to forget: printer ribbons and carbon paper. Ribbons and carbon paper must be disposed of properly. Because of the large variety of ribbons and printers, it is difficult to state with certainty that any and all classified information have been totally obscured from a given ribbon unless you examine that ribbon in detail. Therefore, printer ribbons are controlled at the highest classification of information ever printed by that ribbon until that ribbon is destroyed. The same ribbon is used in the printer for classified and unclassified information consistent with the levels of physical security enforced for the area.

Carbons are easily readable and must be handled and disposed of in accordance with the classification of data they contain. Remember, regardless of what the media is, it must be disposed of in accordance with the *Security Manual* if it ever contained classified information.

Basically, the requirement states that the data must be destroyed beyond recognition. If the media did not contain classified information, follow your activity's standard operating procedures (SOPs).

AIS SECURITY PROGRAM IMPLEMENTATION

The risk analysis and higher authority instructions provide the basis for an AIS security program. Even though implementation of the program depends on local instructions/directives and conditions, it may not be clear just where to begin.

AIS SECURITY PROGRAM PLANNING

Following is a suggested outline to use as a basis for planning an AIS security program:

- **Perform preliminary planning.** Establish an AIS security team to prepare an AIS security program and make responsibility assignments.
- **Perform a preliminary risk analysis.** This will identify major problem areas.
- **Select and implement urgent "quick fix" security measures.** This should be done on an as-needed basis.
- **Perform and document a detailed risk analysis.** This will allow for review and approval.
- **Justify cost and document action plans.** Based on the approved risk analysis selected, develop budgets and schedules for security measures, contingency plans, training and indoctrination plans, and test plans.
- **Carry out the approved action plans.**
- **Repeat the detailed risk analysis and subsequent steps regularly, at least annually.** Conduct more frequently if required based on the results of tests, inspections, and changes in mission or environment.

AIS SECURITY PLAN DOCUMENTATION

Include adequate documentation in the action plans. For example, the documentation might include the following:

- A security policy statement that provides general guidance and assigns responsibilities;
- A security handbook (with instructions) that describes in detail the security program and procedures and the obligations of AIS personnel, users, and supporting personnel;
- Command standards for system design, programming, testing, and maintenance to reflect security objectives and requirements;
- Contingency plans for backup operations, disaster recovery, and emergency response; and
- Booklets or command instructions for AIS staff indoctrination in security program requirements.

Depending on the normal practices of the AIS facility, these documents may be completely separate items or they may be included in other documents. For example, emergency response plans for the AIS facility might be included in the command's Disaster Control Plan. Similarly, security standards could be added to existing documents.

The final point to be made is the importance of continuing the inspection and review of the security program. A major effort is required for the initial risk analysis, but once it is completed, regular review and updating can be done much more quickly. By evaluating changes in command mission, the local environment, the hardware configuration, and tasks performed, the AIS technical manager can determine what changes, if any, should be made in the security program to keep it effective.

AUTHORITATIVE REFERENCES

Numerous higher authority instructions relate to physical security, data protection, and security in general. You should have a thorough knowledge of them before implementing any security plan. Refer to the following instructions and manuals to learn about AIS security and when making security decisions:

- *Department of the Navy Automatic Data Processing Security Program*, OPNAVINST 5239.1 with enclosures;
- *Guideline for Automatic Data Processing Risk Analysis*, FIPS PUB 65 (enclosure 3 to OPNAVINST 5239.1);
- *Department of the Navy Information and Personnel Security Program Regulation*, OPNAVINST 5510.1;
- *Department of the Navy Information Systems Security (INFOSEC) Program*, SECNAVINST 5239.3.

AIS THREATS AND RISK ANALYSIS

First, when designing its security program, a command must look at the potential AIS threats and perform a risk analysis.

AIS THREATS

When planning a security program, the AIS technical manager should be aware of all the types of threats that may be encountered. Not every Navy AIS facility will be faced with each type of threat, especially if the facility is aboard ship. The impact of a given threat may depend on the geographical location of the AIS facility (earthquakes), the local environment (flooding), and potential value of property or data to a thief, or the perceived importance of the facility to activists and demonstrators or subversives. Examples of natural and unnatural threats include:

- Unauthorized access by persons to specific areas and equipment for such purposes as theft, arson, vandalism, tampering, circumventing of internal controls, or improper physical access to information;
- AIS hardware failures;
- Failure of supporting utilities, including electric power, air conditioning, communications circuits, elevators, and mail conveyors;
- Natural disasters, including floods, windstorms, fires, and earthquakes;
- Accidents causing the nonavailability of key personnel;
- Neighboring hazards, such as close proximity to chemical or explosive operations, airports, and high crime areas;
- Tampering with input, programs, and data; and
- The compromise of data through interception of acoustical or electromagnetic emanations from AIS hardware.

The preceding list of threats to the operation of an AIS facility contains only a few of the reasons why each command should have an ongoing security program adapted and tailored to its individual needs and requirements. Not all threats and preventive measures can be discussed in this chapter. However, we will cover the more common threats and remedial measures. For a thorough review of the subject, refer to the *Department of the Navy Physical Security and Loss Prevention,* OPNAVINST 5530.14.

RISK ANALYSIS

The AIS facility upper management should begin development of the security program with a risk analysis. A risk analysis, as related to this chapter, is the study of potential hazards that could threaten the performance, integrity, and normal operations of an AIS facility. Experience at various commands shows that a quantitative risk analysis produces the following benefits:

- Objectives of the security program relate directly to the missions of the command.
- Those charged with selecting specific security measures have quantitative guidance on the type and amount of resources the AIS facility considers reasonable to expend on each security measure.
- Long-range planners receive guidance in applying security considerations to such things as site selection, building design, hardware configurations and procurements, software systems, and internal controls.
- Criteria are generated for designing and evaluating contingency plans for backup operations, recovery from disaster, and dealing with emergencies.
- An explicit security policy can be generated that identifies what is to be protected, which threats are significant, and who will be responsible for executing, reviewing, and reporting the security program.

Loss Potential Estimates

The first step to consider when preparing the risk analysis is to estimate the potential losses to which the AIS facility is exposed. The objective of the loss potential estimate is to identify critical aspects of the AIS facility operation and to place a monetary value on the loss estimate. Losses may result from a number of possible situations, such as:

- **Physical destruction or theft of tangible assets.** The loss potential is the cost to replace lost assets and the cost of delayed processing.
- **Loss of data or program files.** The loss potential is the cost to reconstruct the files, either

from backup copies if available or from source documents and possibly the cost of delayed processing.

- **Theft of information.** The loss potential because of theft is difficult to quantify. Although the command itself would sustain no direct loss, it clearly would have failed in its mission. In some cases, information itself may have market value. For example, a proprietary software package or a name list can be sold.
- **Indirect theft of assets.** If the AIS is used to control other assets, such as cash, items in inventory, or authorization for performance of services, then it may also be used to steal such assets. The loss potential would be the value of such assets that might be stolen before the magnitude of the loss is large enough to assure detection.
- **Delayed processing.** Every application has some time constraint, and failure to complete it on time causes a loss. In some cases the loss potential may not be as obvious as, for example, a delay in issuing military paychecks.

To calculate the loss potential for physical destruction or theft of tangible assets, AIS technical managers and upper management should construct a table of replacement costs for the physical assets of the AIS facility. The physical assets usually include the building itself and all its contents. This tabulation, broken down by specific areas, helps to identify areas needing special attention. While the contents of the typical office area may be valued at $100 to $500 per square foot, it is not unusual to find the contents of a computer room are worth $5,000 to $10,000 per square foot. The estimate is also helpful in planning for recovery in the event of a disaster.

The remaining four loss potential types listed are dependent on the characteristics of the individual data processing tasks performed by the AIS facility. AIS technical managers should review each task to establish which losses a facility is exposed to and which factors affect the size of the potential loss. Call on users to help make these estimates.

To make the best use of time, do a rapid, preliminary screening to identify the tasks that appear to have significant loss potential. An example of preliminary estimates is shown in table 4-1.

Having made a preliminary screening to identify the critical tasks, seek to quantify loss potential more precisely with the help of user representatives familiar with the critical tasks and their impact on other activities. Mishaps and losses that could occur should be considered, on the assumption that if something can go wrong, it will. The fact that a given task has never been tampered with, used for an embezzlement, or changed to mislead management in the command is no assurance that it never will be. At this stage of the risk analysis, all levels of management should assume the worst.

Threat Analysis

The second step of the risk analysis is to evaluate the threats to the AIS facility. Threats and the factors that influence their relative importance were listed earlier in this chapter. Details of the more common threats are discussed later in this chapter and, to the extent it is available, general information about the probability of occurrence is given. Use these data and higher authority instructions/manuals and apply common sense to develop estimates of the probability of occurrence for each type of threat.

Table 4-1.—Example of Preliminary Estimates of Loss Potential

TASK NAME	RUN TIME	FILE RECONSTRUCTION	CLASSIFIED/ SENSITIVE DATA	PRIOR COMPROMISE/ THEFT OF INFORMATION	DELAYED PROCESSING IMPACT	PROJECT	MANPOWER COST ESTIMATE
R	1.5/D	Easy	No	No	Extreme	Payroll	1 day
S	Online	Very Difficult	Yes	Yes	Extreme	Operations	1 day
T	2.0/D	Difficult	Yes	No	Moderate	Inventory	7 days
U	0.5/W	Normal	No	No	Low	Research	6 days
V	0.7/M	Difficult	Yes	No	Very low	Research	2 days
W	4.5/W	Easy	No	No	Moderate	Inventory	0.4 day

While the overall risk analysis should be conducted by the AIS technical manager, other personnel at the AIS facility can contribute to the threat analysis, and their help should be requested. Table 4-2 includes a list of common threats at a shore AIS facility, with space for listing the agency or individual to contact should the need arise. Your AIS facility should have a similar list with local contacts of help and information.

Annual Loss Expectancy

The third step in the risk analysis is to combine the estimates of the value of potential loss and probability of loss to develop an estimate of annual loss expectancy. The purpose is to pinpoint the significant threats as a guide to the selection of security measures and to develop a yardstick for determining the amount of money that is reasonable to spend on each of them. In other words, the cost of a given security measure should relate to the loss(es) against which it provides protection.

To develop the annual loss expectancy, construct a matrix of threats and potential losses. At each intersection, ask if the given threat could cause the given loss. For example, fire, flood, and sabotage do not cause theft-of-information losses; but, in varying degrees, all three result in physical destruction losses and losses because of delayed processing. Likewise, internal tampering could cause an indirect loss of assets. In each case where there can be significant loss, the loss potential is multiplied by the probability of occurrence of the threat to generate an annual estimate of loss.

Remedial Measures Selection

When the estimate of annual loss is complete, AIS upper management will have a clear picture of the significant threats and critical AIS tasks. The response to significant threats can take one or more of the following forms:

- **Alter the environment to reduce the probability of occurrence.** In an extreme case, this could lead to relocation of the AIS facility to a less-exposed location. Alternatively, a hazardous occupancy adjacent to or inside the AIS facility could be moved elsewhere.
- **Erect barriers to ward off the threat.** These might take the form of changes to strengthen the building against the effects of natural disasters,

Table 4-2.—Threat Help List

COMMON THREATS	SOURCES OF LOCAL INFORMATION AND HELP	LOCAL PHONE NUMBER
Fire		
Flood		
Earthquake		
Windstorm		
Power failure		
Air-conditioning failure		
Communications failure		
AIS hardware failure		
Intruders, vandals		
Compromising emanations		
Internal theft		
Internal misuse		

saboteurs, or vandals. (See the *Security Manual* and OPNAVINST 5530.14 for evaluation guidelines.) Special equipment can be installed to improve the quality and reliability of electric power. Special door locks, military guards, and intrusion detectors can be used to control access to critical areas.

- **Improve procedures to close gaps in controls.** These might include better controls over operations or more rigorous standards for programming and software testing.
- **Early detection of harmful situations permits more rapid response to minimize damage.** Fire and intrusion detectors are both typical examples.
- **Contingency plans permit satisfactory accomplishment of command missions following a damaging event.** Contingency plans include immediate response to emergencies to protect life and property and to limit damage, maintenance of plans and materials needed for backup operation offsite, and maintenance of plans for prompt recovery following major damage to or destruction of the AIS facility. The command's Disaster Control Plan should coincide with the AIS facility's contingency plans.

Table 4-3 shows examples of remedial measures for a few threats. When selecting specific remedial measures, use the following two criteria:

1. The annual cost is to be less than the reduction in expected annual loss that could be caused by threats.
2. The mix of remedial measures selected is to be the one having the lowest total cost.

The first criterion simply says there must be a cost justification for the security program-that it returns more in savings to the AIS facility than it costs. This may seem obvious but it is not uncommon for an AIS manager to call for a security measure, to comply with higher authority security instructions and directives, without first analyzing the risks.

The second criterion reflects the fact that a given remedial measure may often be effective against more than one threat. See table 4-3.

Since a given remedial measure may affect more than one threat, the lowest cost mix of measures probably will not be immediately obvious. One possible way to make the selection is to begin with the threat having the largest annual loss potential. Consider possible remedial measures and list those for which the annual cost is less than the expected reduction in annual loss. Precision in estimating cost and loss reduction is not necessary at this point. If two or more remedial measures would cause a loss reduction in the same area, list them all, but note the redundancy. Repeat the process for the next most serious threat and continue until reaching the point where no cost justifiable measure for a threat can be found. If the cost of a remedial measure is increased when it is extended to cover an additional threat, the incremental cost should

Table 4-3.—Example of Remedial Measures by Threat Type

REMEDIAL MEASURES	THREATS				
	Fire	Internal Theft	External Theft	Hurricane	Sabotage
Fire detection system	X				X
Loss control team	X			X	X
Roving guard patrol	X	X	X		X
Intrusion detectors		X	X		X
Personnel screening		X			X
On-site power generator				X	X
Backup plan	X			X	X

be noted. At this point, there exists a matrix of individual threats and remedial measures with estimates of loss reductions and costs, and thus an estimate of the net saving. This is shown graphically in table 4-4.

For each threat (A, B, C, and D), the estimated loss reduction (column 1), the cost of the remedial measure (column 2), and the net loss reduction (column 3) are given in thousands of dollars. By applying remedial measure J to threat A at a cost of $9,000, a loss reduction of $20,000 can be expected (a net saving of $1 1,000). Furthermore, remedial measure J will reduce the threat B loss by $10,000 at no additional cost and the threat C loss by $4,000 at an added cost of only $1,000. Finally, though, it appears that it would cost more than it would save to apply J to threat D. Therefore, J would not be implemented for D. The net loss reduction from J could be expressed as:

$$J(A, B, \& C) = 11 + 10 + 8$$

$$= \$24{,}000 \text{ net loss reduction}$$

The table indicates that J and K have the same reduction effect on threat A. Since K costs more than J, it might, at first glance, be rejected. However,

$$K(A, B, C, \& D) = 5 + 12 + 6 + 2$$

$$= \$25{,}000 \text{ net loss reduction}$$

and

$$J(A, B, \& C) + K(A, B, C, \& D) = -4 + 22 + 9 + 2$$

$$= \$29{,}000 \text{ net loss reduction}$$

Therefore, while J and K are equally effective on threat A, K appears to be more effective than J on the other threats. Further checking shows their combined use results in the greatest overall net loss reduction.

By going through the process just described, using preliminary estimates for cost and loss reduction, you can test various combinations of remedial measures, and thus identify the subset of remedial measures that appears to be the most effective. At this point, review the estimates and refine them as necessary to ensure compliance with higher authority security instructions.

If all the preceding procedures are followed, the following factors will be established and documented:

- The significant threats and their probabilities of occurrence;
- The critical tasks and the loss of potential related to each threat on an annual basis;
- A list of remedial measures that will yield the greatest net reduction in losses, together with their annual cost.

With this information at hand, AIS upper management can move ahead with implementing the AIS security program. Since the analysis of remedial measures will have identified those with the greatest impact, relative priorities for implementation can also be established.

AIS DISASTER PROTECTION

Fires, floods, windstorms, and earthquakes all tend to have the same basic effects on AIS operations. They cause the physical destruction of the facility and its contents and interrupt normal operations. They also represent a threat to the life and safety of the AIS staff. To illustrate the effects of the physical destruction of a facility, we have selected fire safety. Other causes of disasters include the loss of support utilities and breaches of AIS facility physical security.

FIRE SAFETY

Experience over the last two decades demonstrates the sensitivity of AIS facilities to fire damage resulting in disruption of operations. A number of major losses

Table 4-4.—Threat Matrix Table

REMEDIAL MEASURES	THREATS											
	A			B			C			D		
	(1)	(2)	(3)	(1)	(2)	(3)	(1)	(2)	(3)	(1)	(2)	(3)
J	20*	9	11	10	0	10	4	1	8	2	5	-3
K	20*	15	5	12	0	12	6	0	6	4	2	2

* Same effect.

have involved noncombustible buildings. In the cases where vital magnetic media tapes were safeguarded and the computer hardware was relatively uncomplicated, rapid recovery was possible, often in a matter of days. However, if a large computer configuration were destroyed or if backup records were inadequate, recovery could take many weeks or months.

Fire safety should be a key part of the AIS facility's security program. It should include the following elements:

- Location, design, construction, and maintenance of the AIS facility to minimize the exposure to fire damage;
- Measures to ensure prompt detection of and response to a fire emergency;
- Provision for quick human intervention and adequate means to extinguish fires; and
- Provision of adequate means and personnel to limit damage and effect prompt recovery.

Facility Fire Exposure

The first factor to consider in evaluating the fire safety of an AIS facility is what fire exposure results from the nature of the occupancy (material) of adjacent buildings and the AIS facility building. Generally speaking, the degree of hazard associated with a given occupancy (material) depends on the amount of combustible materials, the ease with which they can be ignited, and the likelihood of a source of ignition.

The second and third fire safety factors are the design and construction of the building. Five basic types of construction are described in table 4-5, with their approximate destruction times.

Table 4-5.—Estimated Destruction Time by Fire for Selected Construction Types

TYPE OF CONSTRUCTION	APPROXIMATE DESTRUCTION TIME
Fire Resistant	2 or 3 hours
Heavy Timber	1 plus hours
Noncombustible	1 hour
*Ordinary Construction	Less than 1 hour
Wood Frame	Minutes

*Depends on size of timber used

The actual performance of a building will depend not only on the type of construction, but also on design details, such as:

- Fire walls, which, in effect, divide a structure into separate buildings with respect to fires;
- Fire-rated partitions, which retard the spread of a fire within a building;
- Fire-rated stairwells, dampers, or shutters in ducts; fire stops at the junction of floors, and walls and similar measures to retard the spread of smoke and fire within a building; and
- Use of low-flame spread materials for floor, wall, and ceiling finish to retard propagation of flame.

Understand that this discussion is very simplified. However, consideration of these factors as they apply to an existing or projected AIS facility will help to determine the amount of attention to pay to fire safety. Seek the assistance of a qualified fire protection engineer or local base fire personnel in evaluating the inherent fire safety of the AIS facility and identifying hazards.

The fourth factor in fire safety is the way in which the building is operated. Keep in mind that the inherent fire safety of a building can be rendered ineffective by careless operation; for example:

- Fire doors propped open;
- Undue accumulation of debris or trash;
- Careless use of flammable fluids, welding equipment, and cutting torches;
- Substandard electric wiring;
- Inadequate maintenance of safety controls on ovens and boilers; or
- Excessive concentration of flammable materials (AIS facilities, for example, have a particular hazard from the accumulation of lint from paper operations).

The AIS security program should strive, in coordination with the building maintenance staff, to identify and eliminate dangerous conditions. NOTE: This must be a continuing effort and a consideration in the assignment of security management responsibilities. The security inspection plan should include verification of compliance with established standards.

Fire Detection

Despite careful attention to the location, design, construction, and operation of the AIS facility, there is still the possibility of a fire. Experience shows repeatedly that prompt detection is a major factor in limiting fire damage. Typically, a fire goes through three stages. Some event, such as a failure of electrical insulation, causes ignition. An electrical fire will often smolder for a long period of time. When an open flame develops, the fire spreads through direct flame contact, progressing relatively slowly, with a rise in the temperature of the surrounding air. The duration of this stage is dependent on the combustibility of the materials at and near the point of ignition. Finally, the temperature reaches the point at which adjacent combustible materials give off flammable gases. At this point, the fire spreads rapidly and ignition of nearby materials will result from heat radiation as well as direct flame contact. Because of the high temperatures and volumes of smoke and toxic gases associated with this third stage, fire fighting becomes increasingly difficult and often prevents people from remaining at the fire site.

Given the objective to discover and deal with a fire before it reaches the third stage, one can see the limitation of fire detection that depends on detecting a rise in air temperature. For this reason, the areas in which electronic equipment is installed should be equipped with products-of-combustion (smoke) detectors. Such detectors use electronic circuitry to detect the presence of abnormal constituents in the air that are usually associated with combustion.

In designing an effective fire detection system, consider the following points:

- **Location and spacing of detectors.** The location and spacing of detectors should take into consideration the direction and velocity of air flow, the presence of areas with stagnant air, and the location of equipment and other potential fire sites. Note that detectors may be required under the raised floor, above the hung ceiling, and in air-conditioning ducts as well as at the ceiling. It may also be wise to put detectors in electric and telephone equipment closets and cable tunnels.

- **Control panel design.** The design of the detection control panel should make it easy to identify the detector that has alarmed. This implies that the detectors in definable areas (for example, the tape vault, the east end of the computer room, and administrative offices) should be displayed as a group on the control panel. In other words, when an alarm sounds, inspection of the control panel should indicate which area or zone caused the alarm. Generally, and preferably, each detector includes a pilot light that lights when the detector is in the alarm state. In some cases there should be a separate indicator light at the control panel for each detector. It is also important to see that the alarm system itself is secure. Its design should cause a trouble alarm to sound if any portion of it fails, or if there is a power failure. Take steps to assure the system cannot be deactivated readily, either maliciously or accidentally.

- **Personnel response.** Meaningful human response to the detection and alarm systems is necessary if they are to be of any value. This means the fire detection system should be designed to assure that someone will always be alerted to the fire. Typically, the computer room staff is expected to respond to an alarm from the AIS facility alarm system. A remote alarm should also be located at another point in the building that is occupied at all times, such as the lobby guard post, security center, or building engineer's station. This provides a backup response when the computer area is not occupied. If there is any possibility the remote alarm point will not be occupied at all times, a third alarm point should be located offsite, usually at the nearest fire station or the command's fire department for the facility.

- **Maintenance.** Proper maintenance is essential to the fire detection system. The nature of smoke detectors is such that nuisance alarms may be caused by dust in the air or other factors. Because of this, there is a tendency to reduce sensitivity of the detectors to eliminate nuisance alarms, with the result that detection of an actual fire may be delayed. To ensure proper operation, see that qualified personnel (a vendor representative, building engineer, or Public Works Center personnel) verify correct operation at the time of installation, and at least once each year thereafter. Furthermore, each fault condition should be corrected immediately. Unfortunately, a common tendency is to turn off the fire detection system or silence the alarm bell, creating the danger that there will be no response if a fire should occur.

In addition to alerting personnel to the presence of a fire, the detection equipment can be used to control the air-conditioning system. There is some support for the view that, upon detection, air-handling equipment be shutdown automatically to avoid fanning the flames and spreading smoke. This is not the best plan, as nuisance alarms will result in needless disruption. The preferred technique is to cause the system to exhaust smoke by stopping recirculation, and switching to 100-percent outside air intake and room air discharge. As a rule, this can be done by adjusting air-conditioning damper controls and their interconnection with the fire detection system. However, it may be necessary to modify the air-conditioning system. The use of either technique is at the discretion of command policy.

Fire Extinguishment

Fire extinguishment may be accomplished using one or more of the following four methods:

- **Portable or hand extinguishers.** Operated by military or civil service personnel to help control the fire before it gets out of hand.
- **Hose lines.** Used by military, civil service, or professional fire fighters to attack the fire with water.
- **Automatic sprinkler systems.** Release water from sprinkler heads activated in the temperature range of 135°F to 280°F.
- **Volume extinguishment systems.** Fill the room with a gas that interferes with the combustion process.

To ensure the effectiveness of portable extinguishers, several measures should be observed. Place extinguishers in readily accesssible locations, not in comers or behind equipment. Mark each location for rapid identification; for example, paint a large red spot or band on the wall or around the column above the point where each extinguisher is mounted. It is important for each AIS technical manager to ensure proper inspection in accordance with command policy. Each extinguisher should have an inspection tag affixed to it with the signature of the inspecting petty officer or fire marshal and the inspection date.

In all probability, the AIS facility technical manager will want to establish a first line of defense against fire involvement between the time of notification of, and response by, professional or highly trained firefighters, and will incorporate this as part of the command's Disaster Control Plan. Every command, regardless of size, needs military personnel who are knowledgeable and trained in fire safety. Any practical and effective organization for fire protection must be designed to assure prompt action immediately at the point where a fire breaks out. This usually necessitates every organizational unit or area of a command having a nucleus of key personnel who are prepared, through instruction and training, to extinguish fires promptly in their beginning stage. Such individuals become knowledgeable in specialized fire protection and the systems applicable to the facility in question: how to turn in an alarm, which type of extinguisher to use for which type of fire, and how to use it. Further, such individuals can serve as on-the-job fire inspectors, constantly seeking out, reporting, and correcting conditions that may cause fires. They can help ensure that fire-fighting equipment is properly located and maintained, that storage does not cause congestion that could hamper fire fighting, and that general housekeeping is maintained at a reasonably high level to minimize fire risk.

SUPPORTING UTILITIES PROTECTION

Every Navy AIS facility is dependent upon supporting utilities, such as electric power and air conditioning, and may have to depend on communication circuits, water supplies, and elevators for its operation. Not all commands are self-sufficient; they contract some or all of these utilities from civil sources. In using these utilities, AIS technical managers should consider the probability of occurrence and the effects of breakdowns, sabotage, vandalism, fire, and flooding. These effects can then be related to the needs of the AIS facility as established by the risk analysis.

We have selected electrical power to illustrate support utility protection. Variations of a normal waveform in the electric power supply can affect the operation of AIS hardware. The AIS hardware rectifies the alternating current, filters, and voltage; regulates the resulting direct current; and applies it to the AIS circuitry. The filtering and regulation cannot be expected to eliminate voltage variations beyond a reasonable range. If line voltage is 90 percent or less of nominal for more than 4 milliseconds, or 120 percent or more of nominal for more than 16 milliseconds, excessive fluctuations can be expected in the dc voltage applied to the hardware circuitry. This power fluctuation causes unpredictable results on hardware, logic, and data transfer. These power line fluctuations, referred to as *transients,* are usually caused by inclement weather.

Internally generated transients depend on the configuration of power distribution inside the AIS facility. The effects of internal transients can be minimize by isolating the AIS hardware from other facility loads. Ideally, the computer area power distribution panels should be connected directly to the primary feeders and should not share step-down transformers with other high-load equipment.

The risk analysis should include a complete power transient and failure study. It should also carefully consider the projected growth in particularly sensitive applications (such as real-time or teleprocessing) in projecting future loss potential.

In some cases it may be economically feasible to connect the AIS facility to more than one utility feeder via a transfer switch. If one feeder fails, the facility's load may be transferred to the alternate feeder. This technique is of greater value if the two feeders connect to different power substations.

If the AIS facility is in a remote area, an uninterrupted power supply (UPS) is usually required as a backup power source. The UPS system can be manually or automatically controlled from prime power sources or from the AIS computer site. The typical UPS consists of a solid-state rectifier that keeps batteries charged and drives a solid-state inverter. The inverter synthesizes alternating current for the computer. A simplified block diagram is shown in figure 4-8.

Depending on the ampere-hour capacity of the battery (or batteries), the UPS can support its load for a maximum of 45 minutes without the prime power source. At the same time, it will filter out transients. To provide extra capacity to protect against a failure of the UPS, a static transfer switch can be inserted between the UPS and the computer, as shown in figure 4-9. The control circuitry for the static switch can sense an overcurrent condition and switch the load to the prime power source without causing noticeable transients.

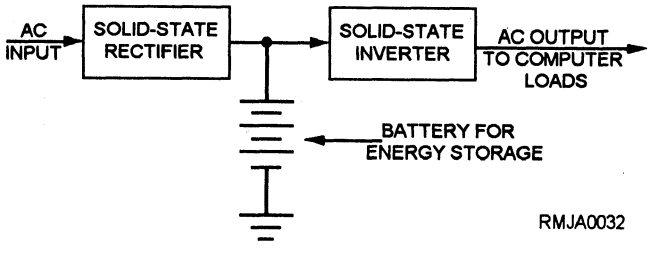


Figure 4-8.—Simplified block diagram of an uninterrupted power supply (UPS).

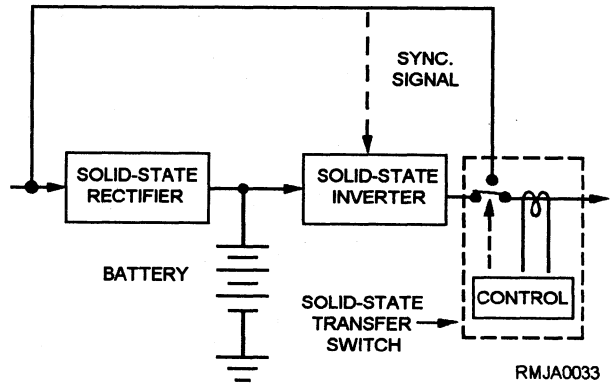


Figure 4-9.—UPS with transfer switch.

If the facility's current needs exceed its UPS capacity, it may be economically feasible to use multiple, independent UPS units, as shown in figure 4-10. Since each unit has its own disconnect switch, it can be switched offline if it fails.

Finally, if the risk analysis shows a major loss from power outages lasting 30 to 45 minutes or beyond, an onsite generator can be installed, as shown in figure 4-11. The prime mover may be a diesel motor or a turbine. When the external power fails, UPS takes over and the control unit starts the prime mover automatically. The prime mover brings the generator up to speed. At this point, the UPS switches over to the generator. Barring hardware failures, the system supports the connected load as long as there is fuel for the prime mover. Note that the generator must be large enough to support other essential loads, such as air conditioning or minimum lighting, as well as the UPS load.

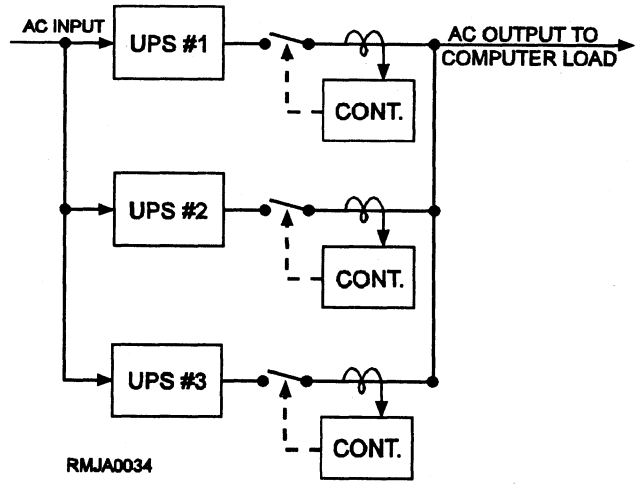


Figure 4-10.—Multiple, independent UPS units.

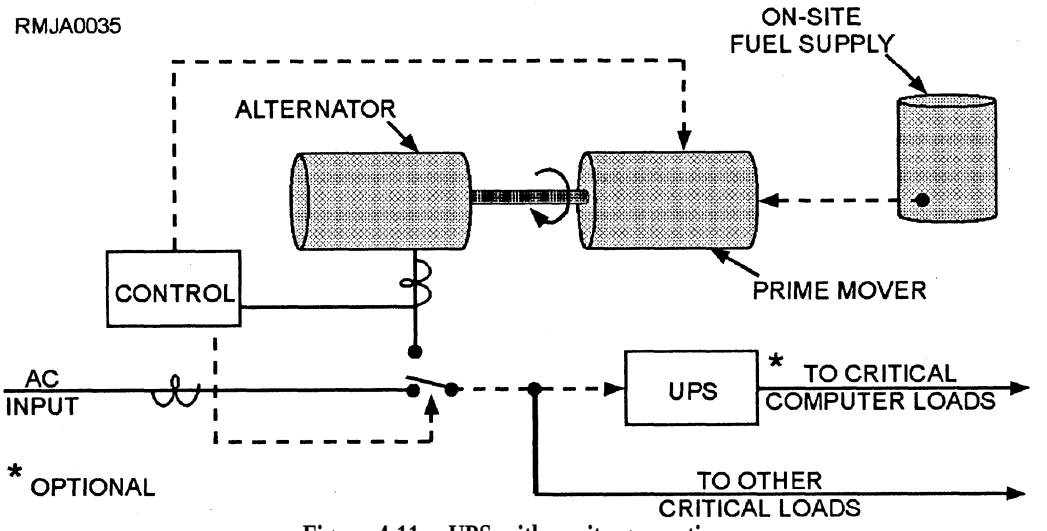


Figure 4-11.—UPS with onsite generation.

When this configuration is used, maintain a close communication liaison with the power plant source to ensure the generator is coming up to normal speed for the switchover from UPS. The UPS system takes over automatically, and the change in power source may not be noticed in the AIS facility. However, when the UPS system changes over to the generator, it may require a manual power panel setting in the AIS facility by the AIS technical manager.

AIS FACILITY PHYSICAL PROTECTION

The physical protection of the AIS facility can be thought of as the process of permitting access to the facility by authorized persons, while denying access to others. The physical protection of an AIS facility is not as stringent for an AIS facility that processes unclassified data as it is for an AIS facility that processes classified data. In the following example/discussion, assume the facility processes classified material and provides physical protection in accordance with OPNAVINST 5510.1 and OPNAVINST 5530.14. Pay particular attention to applying physical protection and security policy wherever AIS equipment is used for processing classified information in accordance with OPNAVINST 5239.1.

Ensure plans are developed for the protection, removal, or destruction of classified material in the case of a natural disaster, civil disturbance, or enemy action. The plans should establish detailed procedures and responsibilities for the protection of classified material so that it does not fall into unauthorized hands in the event of an emergency. Also, indicate what material is to be guarded, removed, or destroyed. An adequate emergency plan for classified material should provide for guarding the material, removing the classified material from the area, complete destruction of the classified material on a phased priority basis, or appropriate combinations of these actions.

The emergency plans should also provide for the protection of classified information in a manner that minimizes the risk of loss of life or injury to AIS personnel. The immediate placement of a trained and preinstructed perimeter guard force around the affected area to prevent the removal of classified material is an acceptable means of protecting the classified material. This action reduces the risk of casualties.

Security requirements for the central computer AIS facility area should be commensurate with the highest classified and most restrictive category of information being handled in the AIS. If two or more computer systems are located in the same controlled area, the equipment comprising each system may be located so that direct personnel access, if appropriate, is limited to a specific system.

Boundary Protection

The threat analysis may indicate the need to protect the property boundary of the AIS facility. This maybe accomplished by installing fences or other physical barriers, outside lighting, or perimeter intrusion detectors, or by using a patrol force. Often a combination of two or more of these will be sufficient. Fences should be 8 feet high with three strands of barbed wire. Fences provide crowd control, deter casual trespassers, and help in controlling access to the entrances; however, they do not stop the determined intruder.

In situations where manpower shortages exist, the fence can be equipped with penetration sensors that should sound an internal alarm only. This type of

physical protection system uses small sensors mounted at intervals on the fence and at each gate.

Emanations Protection

In evaluating the need for perimeter protection, take into account the possibility that electromagnetic or acoustic emanations from AIS hardware may be intercepted. Tests show that interception and interpretation of such emanations may be possible under the right conditions by technically qualified persons using generally available hardware. As a rule of thumb, interception of electromagnetic emanations beyond 325 yards is very difficult. However, if there is reason to believe that a potential exposure to interception exists, seek technical guidance from upper management and the Chief of Naval Operations.

Measures to control compromising emanations are subject to approval under the provisions of *Control of Compromising Emanations,* DOD Directive C5200.19, by the cognizant authority of the component approving security features of the AIS system. Application of these measures within industrial AIS systems is only at the direction of the contracting activity concerned under provisions of the *Security Requirements for Automated Information Systems (AIS's),* DOD Directive 5200.28, and the requirements are to be included in the contract.

Interior Physical Protection

Intrusion detection systems (IDSs) (OPNAVINST 5510.1) provide a means of detecting and announcing proximity or intrusion that endangers or may endanger the security of a command. The use of an IDS in the protective program of a command may be required because of the critical importance of a facility or because of the location or the layout of the command.

Remember, IDSs are designed to detect, not prevent, an attempted intrusion. Thus, a comprehensive security plan must contain appropriate security measures along with procedures for an effective reaction force.

Remote Terminal Areas Protection

The physical and personnel security requirements for the central computer facility area are based upon the overall requirements of the total AIS system. The remote terminal area requirements are based upon the highest classified and most restrictive category and type of material that will be accessed through the terminal under system constraints.

Each remote terminal should be individually identified to ensure required security control and protection. Identify each terminal as a feature of hardware in combination with the operating system.

Before personnel of a component that is not responsible for the overall AIS operation can use a remote device approved for handling classified material, security measures must be established. These security measures are established by the authority responsible for the security of the overall AIS. They are agreed to and implemented before the remote device is connected to the AIS.

DOD component systems may become part of a larger AIS network. The approval and authority to authorize temporary exceptions to security measures for the component's system in the network requires two components. These include the DOD component operating the AIS system and the DOD component having overall responsibility for the security of the network.

Each remote terminal that is not controlled and protected as required for material accessible through it should be disconnected from the AIS system when the system contains classified information. Disconnect procedures are used to disconnect remote input/output terminals and peripheral devices from the system by a hardware or software method authorized by the designated approving authority of the central computer facility.

Security Survey

An annual security survey of the AIS facility area should be conducted by the AIS technical manager. The first step of the survey is to evaluate all potential threats to the AIS facility as discussed earlier in this chapter. The second step is to define and tabulate areas within the facility for control purposes. Details depend on the specifics of each facility, but the following are common areas to consider:

- Public entrance or lobby;
- Loading dock;
- Spaces occupied by other building tenants;
- AIS facility reception area;
- AIS input/output counter area;
- AIS data conversion area;
- Media library;
- Systems analysis and programming areas;
- Computer room spaces;

- Communications equipment spaces; and
- Air conditioning, UPS, and other mechanical or electrical equipment spaces.

The survey should verify security measures already in place and recommend any improvements to upper management. Obtain a current floor plan on which to depict all areas within the facility. Include all access points and any adjacent areas belonging to the AIS facility, such as parking lots and storage areas. Begin the survey at the perimeter of the AIS facility, considering the following:

- **Property line.** Include fencing, if any, and type. Note the condition, the number of openings according to type and use, and how they are secured. Are there any manned posts at the property line?
- **Outside parking facilities.** Are these areas enclosed, and are there any controls? Are parking lots controlled by manned posts or are devices used?
- **Perimeter of facility.** Note all vehicular and pedestrian entrances and what controls are used, if any. Check all doors—their number, how they are secured, and any controls or devices, such as alarms or key card devices. Check for all ground floor or basement windows and how they are secured, screening or bars, for example, and their vulnerability. Check for other entrances, such as vents and manholes. Are they secured and how? Check for fire escapes—their number and locations and accessibility to the interior of the facility from the fire escape (windows, doors, roof). How are accessways secured?
- **Internal security.** Begin at the top floor or in the basement. Check for fire alarm systems and devices. Note the type, location, and number. Where does the alarm annunciate? Check telephone and electrical closets to see if they are locked. Are mechanical and electrical rooms locked or secured? Note any existing alarms as to type and number. Determine the number and locations of manned posts, hours, and shifts.
- **Monitoring facility.** Know the location, who monitors, who responds, its type, and the number of alarms being monitored.

Table 4-6 is a checklist of other questions that should be asked in the survey.

Table 4-6.—Secunty Measures Checklist

No.	Security Measure	Status
1.	Is the facility/building protected by (an) alarm system(s)?	
2.	How many zones of protection are within the protected building?	
3.	Is the alarm system adequate and does it provide the level of protection required?	
4.	Are there any vulnerable areas, perimeter, or openings not covered by an alarm system?	
5.	Is there a particular system that has a high nuisance alarm rate?	
6.	Is the alarm system inspected and tested occasionally to ensure operation?	
7.	Is the system backed up by properly trained, alert protection personnel who know what steps to take in case of an alarm?	
8.	Is the alarm system regularly inspected for physical and mechanical deterioration?	
9.	Does the system have tamper-proof switches to protect its integrity?	
10.	Is there an environmental or protective housing or cover on the system(s)?	
11.	Is there an alternate or separate source of power available for use on the system in the event of an external power failure?	
12.	Where is the annunciating unit located—local, central station, or remote?	
13.	Who maintains the equipment and how is it maintained (contract, lease equipment, force account personnel, military, or civil service)?	
14.	Is the present equipment up-to-date?	
15.	Are records kept of all alarm signals received, including the time, date, location, action taken, and cause of the alarm?	
16.	Are alarms generated occasionally to determine the sensitivity and the capabilities of systems?	

When the security survey is complete, it provides a picture of the existing alarm systems and the location of each. It also shows the number and location of manned posts, the number of personnel at these posts, and the schedule of each.

With these facts in hand, the AIS technical manager can evaluate existing access controls and protection measures, identify areas where remedial measures are needed, and select specific measures.

Always consider the use of various types of security hardware devices to augment the existing personnel protective force. Through the use of such devices, it may be possible to save on operating cost.

CONTINGENCY PLANNING

Operation plans and the command's organizational manual are prepared and executed for the accomplishment of the command's specific mission. These operation plans assume normal working conditions, the availability of command resources and personnel, and a normal working atmosphere. Despite careful use of preventive measures, there is always some likelihood that events will occur that could prevent normal operations and interfere with the command accomplishing its mission. For this reason, contingency plans are included in the AIS security program. For the purpose of this chapter, we refer to these contingency plans as the Continuity of Operations Plan (COOP).

Three different types of contingency plans makeup a COOP security program for an AIS facility:

- **Emergency response.** There should be procedures for response to emergencies, such as fire, flood, civil commotion, natural disasters, bomb threats, and enemy attack, to protect lives, limit the damage to naval property, and minimize the impact on AIS operations.
- **Backup operations.** Backup operation plans are prepared to ensure essential tasks (as identified by the risk analysis) can be completed subsequent to disruption of the AIS and that operations continue until the facility is sufficiently restored or completely relocated.
- **Recovery.** Recovery plans should be made to permit smooth, rapid restoration of the AIS facility following physical destruction or major damage.

Each AIS facility should establish and appoint members to a formal board to construct, review, and recommend command procedures for approval in creating a COOP program. Figure 4-12 shows suggested tasks and how they may be set up and assigned. Each AIS facility will need to adapt to its own special circumstances and make full use of the resources available to it.

EMERGENCY RESPONSE PLANNING

The term *emergency response planning* is used here to refer to steps taken immediately after an emergency occurs to protect life and property and to minimize the impact of the emergency. The risk analysis should be reviewed by the AIS technical manager to identify emergency conditions that have particular implications for AIS operations, such as protection of equipment during a period of civil commotion and subsequent to a natural disaster (fire or flood, for example). Where civil commotion and natural disaster are found, local instructions should be developed and implemented to meet the special needs of the AIS facility. These instructions and procedures may be designated the "Loss Control Plan" and implemented as part of COOP.

Loss control can be particularly important to the AIS facility. In a number of recent fires and floods, the value of being prepared to limit damage is amply demonstrated. By reviewing operations and the locations of critical equipment and records with shift leaders, the AIS technical manager can develop measures to use in case of an emergency. The guidelines should be similar to the following:

1. Notify online users of the service interruption.
2. Terminate jobs in progress.
3. Rewind and demount magnetic tapes; remove disk packs.
4. Power down AIS hardware and cover with plastic sheeting or other waterproof material.
5. Put tapes, disks, run books, and source documents in a safe place.
6. Power down air-conditioning equipment.

If evacuation of work areas is ordered or likely, instruct all personnel to:

RMJA0036

	COOP BOARD MEMBERS						
	AIS Technical Manager	User Representatives	CO XO GS Upper Management	Security Officer	Supply Division	Public Works Center	Operations Officer (AIS)
1. Establish board members	*		*				*
2. Estimate recovery time	*				*	*	*
3. Failure mode analysis							
AIS hardware	*						*
Utility failure	*			*			*
Fire, flood, wind	*			*			*
4. Loss potential	*	*	*				*
5. Emergency response plans	*		*	*			*
6. Selection of backup modes	*	*	*				*
7. Recovery plans	*	*	*		*	*	*

Figure 4-12.—Organization and tasks for COOP.

1. Put working papers and other unclassified material in desks or file cabinets and close them.
2. Turn off equipment, but leave room lights on.
3. Close doors as areas are evacuated, but ensure that locks and bolts are not secured.

The loss control plan should define the steps to be taken, assign responsibilities for general and specific steps, and provide any needed materials and equipment in handy locations. In some cases, ample time will be available to take all measures, but in extreme emergencies, life safety will dictate immediate evacuation. For this reason, the loss control plan should designate one or more individuals in each AIS area who, in the event of an emergency, will determine what can be done to protect equipment and records without endangering life, and direct AIS staff members accordingly.

Earlier in this chapter, we discussed measures to protect the facility against the effects of fire. Semiannually, review the protective plans with the operations division officer to assure that all normal requirements and any special requirements of the AIS facilities are satisfied. At the same time, brief upper management on the AIS facility plans and status, to get their advice and to ensure good coordination.

When emergency response planning is completed and approved, it should be documented succinctly for easy execution. See figure 4-13.

COOP BACKUP PLANNING

The risk analysis should identify those situations in which backup operations will probably be needed to avoid costly delays in accomplishing the command mission. The next step is to develop plans for backup operations, which are economically, technically, and operationally sound. Details will depend on circumstances at the AIS facility, but some general guidance and suggestions can be helpful in considering the alternatives.

Backup operations may take place onsite when there is only a partial loss of capability. However, they may require one or more offsite locations when there is major damage or destruction. The backup procedures may replicate normal operation or be quite different. When considering backup, AIS management will often find that an exact replica of the onsite AIS system is not available for backup or the time available per day is less than the amount needed to complete all assigned tasks. From this, you might conclude that backup is impossible. On the contrary, a number of things can be done to make backup resources available. The following are examples:

- **Postpone the less urgent tasks.** Tabulate the AIS tasks in descending order of urgency as identified by the risk analysis. Having estimated the time to return to normal following a disruptive event, AIS management can quickly see which tasks can be set aside. These include such things as program development, long cycle (monthly, quarterly, or annual) processing, and long-range planning. As long as adequate catch-up time is available after the return to normal, there should be a number of tasks that can be safely postponed.

FIRE EMERGENCY RESPONSE

1. Report fire (list phone number).
2. Assess life-safety hazard.
3. Evacuate facility if necessary.
4. Initiate loss control procedures.

Figure 4-13.—Fire emergency response.

- **Substitute other procedures.** If increased cost or degraded service can be accepted temporarily, it may be possible to use other procedures. If printer capability is lost, print tapes could be carried to a backup facility for offline printing. It might also be possible to substitute batch processing for online processing temporarily. In some cases, where compatible hardware is not available, it maybe feasible to maintain a second software package that is functionally identical to the regular package but technically compatible with the offsite AIS hardware that is available for backup use.
- **Modify tasks to reduce run time.** To stretch available backup resources, it might be feasible to eliminate or postpone portions of a task, such as information-only reports or file updates that are not time urgent. In some cases, it might help to double the cycle time for a task; that is, run a daily task every other day instead.

By considering these possibilities for each task, the AIS technical manager can develop the specifications for the minimum backup requirements (AIS hardware, resources, and hours per day necessary for adequate backup).

To evaluate alternate backup modes and offsite facilities, consider such factors as:

- AIS hardware usage;
- Transportation of military and civil service personnel with needed supplies and materials;
- Maintenance personnel at the offsite location; and
- Overtime cost factor for civil service personnel.

As these factors come into focus—identification of critical tasks, specific backup modes, and usable offsite AIS facilities-the outlines of the optimum backup plan will begin to emerge. In general, it is wise to form several COOP backup plans; for example:

- **A minimum duration plan.** A plan for backup operation that is not expected to extend much beyond the cause of delay which forces a shift to backup operation; namely, a minimum duration plan that would probably include only the most time urgent AIS tasks.
- **A worst-case plan.** A plan for backup operation for as long as it takes to reconstruct the AIS facility after total destruction.

- **In-between plans.** Plans for one or more operating periods between minimum duration and worst case.
- **A plan for each major partial failure mode.**

While the individual COOP plans are geared to different objectives, they can usually be constructed from a common set of modules. It is often most effective to make a detailed plan for total destruction since this is the most demanding situation. Scaled-down versions or individual elements from this plan can then be used for the less-demanding situations.

Each COOP backup plan should cover the following five basic areas:

- **Performance specifications.** This is a statement of the specific ways in which performance of each task departs from normal; for example, tasks postponed, changes in cycle times, and schedules.
- **User instructions.** Backup operation may require users to submit input in different forms or to different locations or may otherwise call for altered procedures. These should be clearly spelled out to avoid confusion and wasted motion.
- **Technical requirements for each AIS task.** Backup operation of an AIS task will require the availability at the offsite AIS facility of the following items: current program and data files, input data, data control and operating instruction (which may differ from normal instruction), preprinted forms, carriage control tapes, and the like. These requirements must be documented for each task. Procedures also need to be established to ensure the materials needed for backup operation are maintained offsite on a current basis.
- **Computer system specifications.** One or more offsite computer systems are selected for backup operation. The following information should be recorded for each system: administrative information about the terms of backup use, the location of the system, the configuration and software operating system, a schedule of availability for backup operation, and the tentative schedule of AIS tasks to be performed on the system.
- **Administrative information.** It is probable that COOP backup operation will require special personnel assignments and procedures, temporary employment or reassignment of personnel, use of special messengers, and other departures from normal. Details are to be documented, along with guidance on obtaining required approvals.

When each of the COOP backup plans is completed, it should include full documentation and have upper management approval. Each of the plans may have considerable duplication. However, it is suggested that each plan be completely documented to be sure nothing has been overlooked.

RECOVERY PLANNING

The use of a backup facility usually means both extra expense and degraded performance. Therefore, give some thought to recovery by developing and maintaining supporting documents that minimize the time required for recovery. Furthermore, the AIS staff will be hard pressed by backup operations. If others can handle recovery, the workload on the AIS staff will be reduced during the emergency and the process will undoubtedly be carried out more effectively and economically. Recovery from total destruction requires the following tasks be completed:

- Locate and obtain possession of enough floor space to house the AIS facility with a live-load capacity as required by the AIS hardware and suitably located with respect to users and AIS staff spaces.
- Perform required modifications for needed partitions, raised floor, electric power distribution, air conditioning, communications, security, fire safety, and any other special requirements.
- Procure and install AIS hardware.
- Procure needed supplies, office equipment and furniture, tape storage racks, decollators, and so forth.
- Verify that all needed hardware, equipment, and materials are on hand and in good working order. Then transfer operations from the backup site to the reconstituted AIS facility.

If the necessary documents have been prepared and stored offsite before the emergency, it should be possible for all but the last tasks to be completely

reconstructed with minimum effort. Figure 4-14 shows a simplified step diagram of a normal reconstruction effort.

COOP TESTING

Because emergencies do not occur often, it is difficult to assure adequacy and proficiency of personnel and plans without regular training and testing. Therefore, it is important to plan and budget for both. The availability of needed backup files may be tested by attempting to repeat a particular task using onsite hardware but drawing everything else from the offsite location. Experience demonstrates the value of such tests in validating backup provisions; it is not uncommon to discover gross deficiencies despite the most careful planning. Compatibility with the offsite facility should be verified regularly by running one or more actual tasks. A number of AIS facilities conduct such tests as a part of an overall inspection.

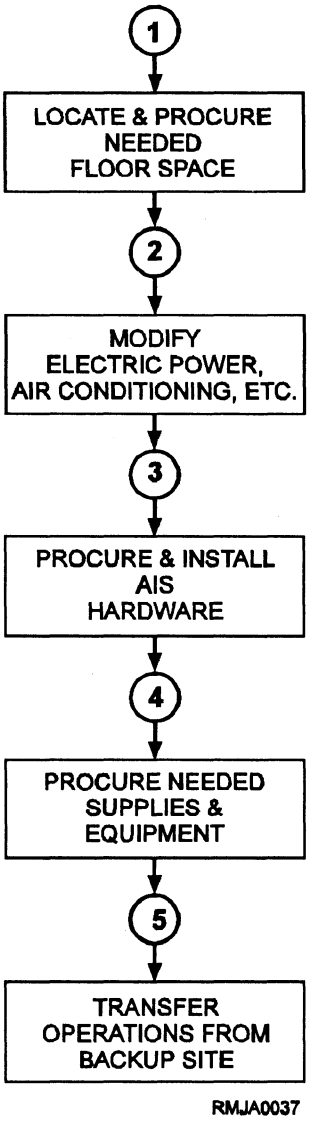


Figure 4-14.—Simplified diagram of an AIS facility

Similar tests of procedures for fire fighting, loss control, evacuation, bomb threat, and other emergencies will give assurance that plans are adequate and workable. At the same time. they provide an opportunity for training AIS personnel. Each test should have a specific objective. A team should be assembled to prepare a scenario for the test, to control and observe the test, and to evaluate the results. This evaluation provides guidance for modifications to emergency plans and for additional training. The important point is to be sure the emergency plans do, in fact, contribute to the security of the AIS facility.

SECURITY INSPECTIONS

The final element of the AIS security program for every naval AIS facility should be a review or inspection process. The inspection should be an independent and objective examination of the information system and its use (including organizational components) and including the following checks:

- Checks to determine the adequacy of controls, levels of risks, exposures, and compliance with standards and procedures; and
- Checks to determine the adequacy and effectiveness of system controls versus dishonesty, inefficiency, and security vulnerabilities.

The words *independent* and *objective* imply the inspection complements normal management inspections, visibility, and reporting systems and is neither a part of, nor a substitute for, any level of management.

What can an inspection be expected to accomplish? First, it evaluates security controls for the AIS facility. Second, it provides each level of management an opportunity to improve and update its security program. Third, it provides the impetus to keep workers and management from becoming complacent. Fourth, if done effectively, it tends to uncover areas of vulnerability. Remember, risks change, and new threats arise as systems mature.

Major factors to consider in determining the frequency of internal inspections include the frequency of external inspections, the rate of change of the AIS, the amount and adequacy of controls, the threats that face the facility, the results of previous inspections, and the directions of higher authority. Inspection activity, direction, and implementation are usually at the discretion of the commanding officer of the command with jurisdiction over the AIS facility.

INSPECTION PREPARATION

The inspection should be conducted by some department or facility outside the span of control of the AIS technical manager. One of the main principles in selecting an inspection team is that members should not be responsible for AIS operations. Team members should have some knowledge of data processing and, if possible, basic inspection principles. A programming or AIS operations background is desirable but not essential. An experienced military or civil service user of AIS services might have the necessary qualifications. The role of the team is not to develop security controls, but to evaluate established controls and procedures. Also, the team should not be responsible for enforcing control procedures, which is clearly an AIS management responsibility.

The character of each of the inspection team members is extremely important. Judgment, objectivity, maturity, ability, and a probing nature will all affect the success of the inspection. The leader of the inspection team must be able to organize the efforts, prepare a good written report, and communicate findings effectively. The leader should be an officer, warrant officer, chief petty officer, or U.S. civilian employee who is GS-7 or above. If not technically oriented, the team leader should be assisted by someone whose technical judgment and knowledge of AIS is reliable.

The size of the team depends upon the size of the facility and the scope of the inspection. A large facility should consider including personnel from the following areas on the inspection team:

- **Internal inspection.** The knowledge and discipline to conduct an inspection can be provided through internal inspection specialists. Inquisitiveness, a probing nature, and attention to detail are typical characteristics desired for inspection board members. Even though an inspection team member generally is not trained in data processing technology, it should not be difficult to appoint team members with some data processing knowledge.
- **Security.** A security officer is a welcome addition to an inspection team.
- **Computer operations.** Technical expertise in data processing is required. Both programming knowledge and operations experience is helpful. Perhaps the data processing internal security officer has these skills and, if so, should be a prime candidate for the team. Using someone from the *AIS* facility being evaluated need not significantly affect the objectivity of the inspection process.
- **Users.** Users have the most to gain from an effective inspection because of their dependence on the AIS facility, yet too often they have little or no interest in AIS controls or security measures. To encourage participation in the AIS security program, one or more users who are concerned about sensitive data being compromised, disclosed, or destroyed should be motivated to join or should be appointed to the inspection team.
- **Building management.** Many of the physical security controls to be inspected—fire prevention and detection, air conditioning, electric power, access controls, and disaster prevention-relate to building management and engineering.
- **Outside specialists.** Independent, experienced viewpoints provided by outside consultants can be very helpful.

The composition of the team can be flexible. One of the prime requirements is that it consist of people who are objective. If only one AIS facility is to be inspected, the members of the team can be assigned for the term of the inspection and then returned to their normal jobs. If there are many AIS facilities under the jurisdiction of the command, it might be advisable to establish a permanent inspection team to review all facilities on a recurring basis. In any event, the composition of the team should be changed periodically to bring in fresh viewpoints and new and different inspection techniques.

THE INSPECTION PLAN

A comprehensive inspection plan must be developed to properly conduct an internal inspection of security. It should be action-oriented, listing actions to be performed. The plan must be tailored to the particular facility. It should include the report and report formatting requirement and the distribution of the final report. This means quite a bit of work is required in its development.

The first step is to examine the security policy for the AIS facility. This policy may apply to an entire naval district, a command, a ship, a department, or a single AIS facility. In any case, the security policy should be reviewed and pertinent security objectives extracted for subsequent investigation. The next step is to review the risk analysis plan, identifying those

vulnerabilities that are significant for the particular facility. Third, the AIS Facility Security Manual, the Operations Manual, and other appropriate documents should be reviewed to determine what the specified security operating procedures are. And last, the AIS facility organization chart and job descriptions should be examined to identify positions with specific security or internal control responsibilities. This background material forms the basis for the development of the inspection plan. A number of general questions should be considered when formulating the inspection program. The following are examples:

- **What are the critical issues with regard to security?** Does the AIS facility process classified or otherwise sensitive data? Does the processing duplicate that of other data centers, thereby providing some sort of backup or contingency capability? Or is it a stand-alone activity processing unique applications? What are the critical applications in terms of the inspection emphasis?

- **What measures are least tested in day-to-day operations?** For example, if the computer fails every day at 1615 because of power switchovers, the immediate backup and recovery requirements are likely to be well formulated and tested. However, the complete disaster recovery plan probably has not been tested, unless there is a specific policy to do so. This is a key point. Security measures of this type are often inadequately exercised.

- **What inspection activities produce the maximum results for least effort?** A test of fire detection sensors under surprise conditions tests not only the response to alarms but also the reaction of the fire party and the effectiveness of evacuation plans. In interviewing personnel, the team should design questions to elicit comprehensive answers. For example, the question "How would you process an unauthorized job?" is likely to elicit more information than "Are job authorization controls effective?" The most likely answer to the second question is a simple and uninformative "Yes."

- **What are the security priorities?** Because of particular policy, a request for an investigation, or an incident of loss, interruption, or compromise, the testing of a particular security measure probably should receive more emphasis than another equally important but noncurrent topics. One must, however, avoid irrational concentration on anyone aspect of the program. Management overemphasis as a result of a recent security breach should be tempered with a rational approach toward investigating all aspects of computer security.

Another step in the process of developing an inspection plan is the review of previous inspection reports. Many times these identify weaknesses or concerns that should have been corrected, and so should bean item of special attention in the current inspection.

CONDUCTING INSPECTIONS

Advantages can be gained from using both scheduled and surprise inspections. A scheduled inspection should meet the general policy requirements of the particular facility and should occur at least annually. This could be a major inspection conducted by an outside command, an internal inspection, or a spot check inspection to review specialized items of interest, perhaps as a result of previous inspection reports of findings. The distinguishing characteristic is that it is scheduled in advance, with a resultant flurry of preparation by the AIS facilities. It motivates cleaning up loose ends, but limits what can really be learned from the inspection.

A surprise inspection is designed to test on a no-notice basis certain elements of security and control. It should be approved by the commanding officer of the command in charge of the AIS facility. It can be accomplished by the command or an external inspection team. It can be used to test those elements best reviewed on a surprise basis, such as fire response, access control, and personnel complacency.

When a scheduled inspection is conducted, the first step normally is to interview AIS personnel. Generally, the first walk-through includes interviews with the AIS technical manager. Searching questions, rather than leading questions, should be the rule, and the best approach is to allow the interviewee to talk as freely as possible. If you are the interviewer, ask questions to put the interviewees in the position of probing for their answers. For example, "What is your biggest access control problem?" not "Do your people wear badges?" Ask how illegal entry or sabotage would be accomplished. Do not hesitate to ask the same questions of more than one person. It is interesting how varied the responses can be.

The conduct of the interviewer is important. Strive to be open in dealing with interviewees. Avoid allusions to private information and obscure references

to other people or events or in any other way cultivating an air of mystery or superiority. It goes without saying the use of good human relations techniques is essential to a successful interview. Nothing can be gained by being belligerent and antagonizing the interviewee. Your conduct should be firm and inquisitive, but also calm, sincere, and open. Probe in some detail any answer that appears evasive or defensive.

Taking notes is a matter of individual preference. Some people take very adequate notes at listening speed. Others must devote all their attention to listening. If note taking is a problem, the interview could be conducted by two-person teams. Another alternative is to use a portable tape recorder, making certain the interviewee knows in advance that the interview is being taped. If a two-person team or a tape recorder is not available, attempt to listen and absorb as much as possible, then record notes and impressions directly after the conclusion of the interview.

The evaluation tests can be scheduled or come as a surprise. Most security inspections include testing the emergency, fire, evacuation, and disaster recovery activities. Access controls should also be tested on a no-notice basis. Tests are best scheduled or conducted early in the inspection rather than after everyone is alerted to the presence of the inspection team. Special concern, guidance, and instructions must be taken into consideration when the AIS facility has armed guards. It is possible to test the adequacy of programmed controls and data authorization by submitting jobs that attempt to bypass these controls. Take care not to destroy live data. However, if AIS upper management believes error detection and correction controls really work, then there should be no objection to the introduction of deliberate errors to test these controls.

The inspection team should convene periodically, preferably at the end of each day's activity, to review progress and to compare notes. Areas of weakness or concern should be highlighted, and additional tests or interviews scheduled to investigate further any particular areas of concern. Copies of the inspection working paper should be classified, numbered, dated, and organized for ease of understanding, review, and comparison.

At the completion of the inspection, a written report is to be prepared immediately, while impressions are still fresh. As a rule, the inspection report includes:

- An executive summary;
- A description of the inspection—dates locations, scope, objectives, and so forth;
- A detailed report of observations made;
- Conclusions drawn from the observations; and
- Recommendations for corrective actions, as appropriate.

The degree of cooperation received should be noted and favorable conclusions should be given the same prominence as deficiencies. Tables, charts, and matrices of results, statistical tests, and conclusions may be very helpful. Distribute the final report to the AIS facility and the command upper management as prescribed in the planning phase.

INSPECTION FOLLOW-UP

An inspection is of little use unless it is the basis for improvement, correction, and management follow-up. The responsibility for implementation of such activity normally resides with the commanding officer (CO) of the command. The CO must, in turn, assign responsibilities for corrective action. The best approach is to summarize each major deficiency on a control sheet, outlining requirements, problem definition, responsibility, action taken or required, and follow-up action. In addition, an indication should be made of the date that action should be completed, or if it is to continue. Some of the corrective action may require additional funds; this should be noted.

Corrective action, follow-up, and disposition of the deficiencies should follow a recurring reporting cycle to upper management. Quarterly reports are recommended for any inspection control items still open.

The final step is a frank and honest evaluation of the inspection itself by AIS facility management and the inspection team. A group discussion should be held with the expressed purpose of improving future inspection procedures and processes. The inspection plan may need to be amended or the team composition may need to be changed. The emphasis of the inspection should always be positive—one of helping AIS management at all levels to improve the security and control of the AIS facility.

DATA PRIVACY

The Privacy Act of 1974 (Public Law 93-579) imposes numerous requirements upon naval commands to prevent the misuse or compromise of data concerning individuals. Navy AIS facilities that process personal data must provide a reasonable degree of protection against unauthorized disclosure, destruction, or

modification of personal data, whether it is intentional or results from an accident or carelessness.

Department of the Navy Information Systems Security (INFOSEC) Program, SECNAVINST 5239.3, provides guidelines for use by all Navy organizations in implementing any security safeguards that they must adopt to implement the Privacy Act. It describes risks and risk assessment, physical security measures, appropriate information management practices, and computer system/network security controls.

Department of the Navy Privacy Act (PA) Program, SECNAVINST 5211.5, implements the Privacy Act and personal privacy and rights of individuals regarding their personal records. It delineates and prescribes policies, conditions, and procedures for the following:

- Any Department of the Navy system of records possessing a record on an individual must verify it has the record upon the request of the individual.
- The identity of any individual requesting personal record information maintained on them must be confirmed before the information is released.
- An individual must be granted access to his/her personal files on request.
- Any request from an individual concerning the amendment of any record or information pertaining to the individual for the purpose of making a determination on the request or appealing an initial adverse determination must be reviewed.
- Personal information is collected, safeguarded, and maintained, and decisions are made concerning its use and dissemination.
- The disclosure of personal information, and decisions concerning which systems records are to be exempted from the Privacy Act.
- Rules of conduct are established for the guidance of Department of the Navy personnel who are subject to criminal penalties for noncompliance with the Privacy Act.

The Chief of Naval Operations is responsible for administering and supervising the execution of the Privacy Act and SECNAVINST 5211.5 within the Department of the Navy. Additionally, the Chief of Naval Operations is designated as the principal Privacy Act coordinator for the Department of the Navy.

The major provisions of the Privacy Act that most directly involve computer security are found in the following parts of title 5, United States Code (U.S.C.), section 552a:

1. Subsection (b)—limits disclosure of personal information to authorized persons and commands.
2. Subsection (e)(5)—requires accuracy, relevance, timeliness, and completeness of records.
3. Subsection (e)(10)—requires the use of safeguards to ensure the confidentiality and security of records.

The following terminology is used in discussing the treatment of personal data:

- **Confidentiality.** A concept that applies to data. It is the status accorded to data that requires protection from unauthorized disclosure.
- **Data integrity.** The state existing when data agrees with the source from which it is derived, and when it has not been either accidentally or maliciously altered, disclosed, or destroyed.
- **Data Security.** The protection of data from accidental or intentional, but unauthorized, modification, destruction, or disclosure.

Safeguards that provide data protection are grouped into three categories: physical security measures, information management practices, and computer system/network security controls. Specifically, these are:

- **Physical security measures.** Measures for protecting the physical assets of a system and related facilities against environmental hazards or deliberate actions as discussed earlier in this chapter.
- **Information management practices.** Procedures for collecting, validating, processing, controlling, and distributing data.
- **Computer system/network security controls.** Techniques available in the hardware and software of a computer system or network for controlling the processing of and access to data and other assets.

Technological safeguards for security risks are presented in figure 4-15. They may be viewed in relation to the control points within a computer

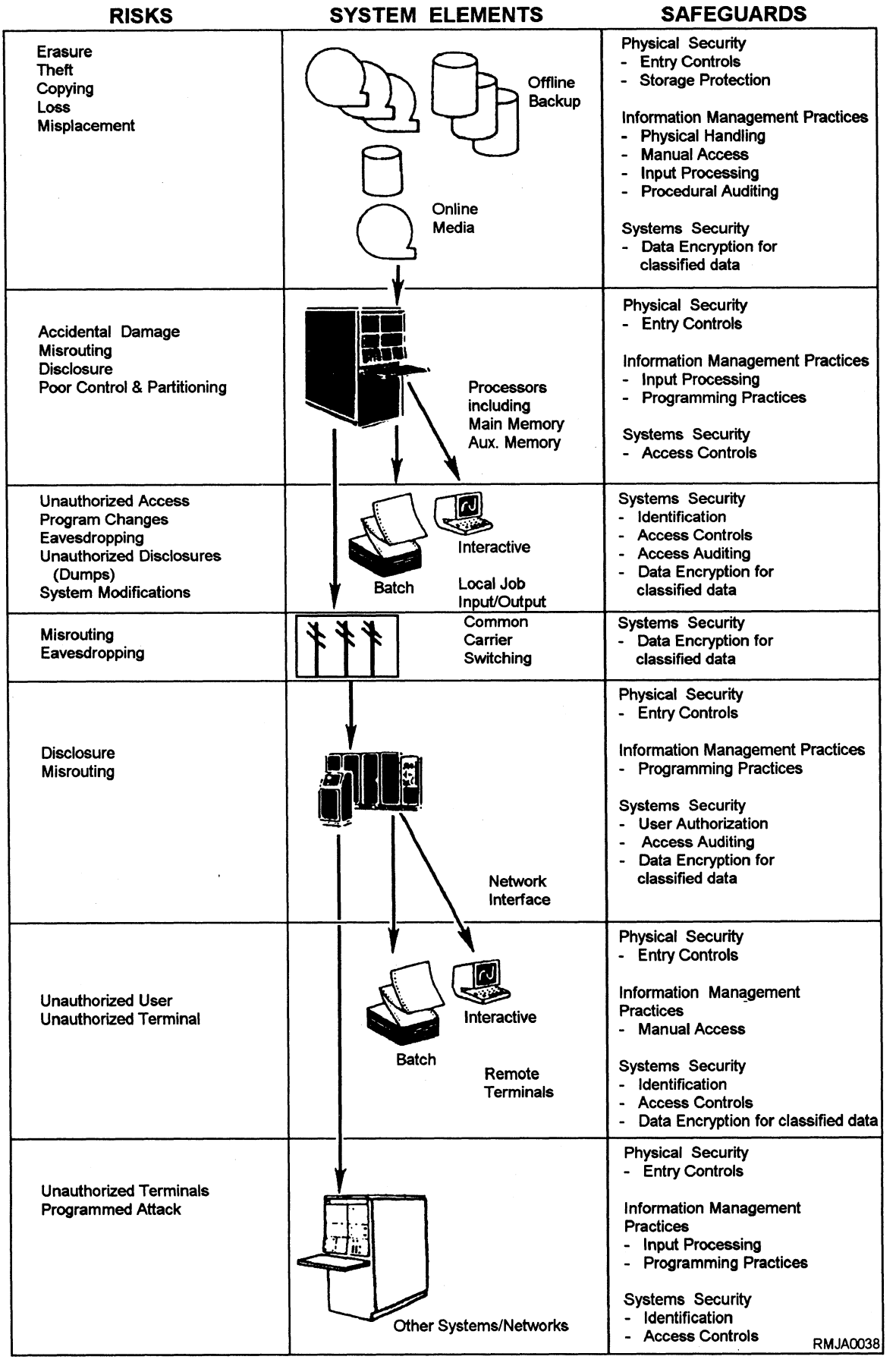


Figure 4-15.—Personal data security risks and technological safeguards.

system/network. This perspective shows the elements of a computer system/network, beginning with the offline storage of personal data in machine-readable media (for example, tapes and disks) and progressing through the many possible processing modes. It includes the use of interactive computer terminals at local and remote locations and the linking of local systems via communications networks. It stresses the value of physical security measures and information management practices, in relation to computer system/network controls.

PERSONAL DATA RISK ASSESSMENT

The first step toward improving a system's security is to determine its security risks using the criteria discussed earlier in this chapter. A personal data security risk assessment benefits a command in three ways:

- It provides a basis for deciding whether additional security safeguards are needed for personal data.
- It ensures that additional security safeguards help to counter all the serious personal data security risks.
- It saves money that might have been wasted on safeguards that do not significantly lower the overall data risks and exposures.

The goal of a risk assessment is to identify and prioritize those events that would compromise the integrity and confidentiality of personal data. The seriousness of a risk depends both on the potential impact of the event and its probability of occurrence.

In general, the risk assessment should consider all risks, not just risks to personal data. While this section of the chapter emphasizes the security of personal data, it is best to develop an integrated set of security safeguards and requirements that protect all classified and other valuable data in the system wherever possible.

The risk assessment should be conducted by a team which is fully familiar with the problems that occur in the daily handling and processing of the personal information. The participants on the risk assessment team should include:

- A representative of the operating facility supported by or having jurisdiction over the data under consideration;
- The programmer responsible for support of the operation or function under consideration;
- A representative from the facility responsible for managing AIS operations;
- A system programmer (if the command has system programmers in a separate fictional area);
- A computer specialist assigned the responsibility for overseeing or inspecting system security; and
- The individual responsible for security.

PERSONAL DATA SECURITY RISKS

Each command should identify its specific risks and evaluate the impact of those risks in terms of its information files. Experience indicates the most commonly encountered security risks are usually accidents, errors, and omissions. The damage from these accidental events far exceeds the damage from all other personal data security risks. Good information management practices are necessary to reduce the damage that can result from these occurrences. Personal data security risks include:

- **Input error.** Data may not be checked for consistency and reasonableness at the time they are entered into the system; or data may be disclosed, modified, lost, or misidentified during input processing.
- **Program errors.** Programs can contain many undetected errors, especially if they were written using poor programming practices or were not extensively tested. A program error may result in undesirable modification, disclosure, or destruction of sensitive information.
- **Mistaken processing of data.** Processing requests may update the wrong data; for example, a tape mounted at the wrong time.
- **Data loss.** Personal data on paper printouts, magnetic tapes, or other removable storage media may be lost, misplaced, or destroyed.
- **Improper data dissemination.** Disseminated data may be misrouted or mislabeled, or it may contain unexpected personal information.
- **Careless disposal of data.** Personal data can be retrieved from wastepaper baskets, magnetic tapes, or discarded files.

Every AIS facility's technical manager and upper management should establish strict controls and procedures over individuals authorized to access the personal data files. If everyone at the facility needs authority to access personal data files, the security measures should adequately control system access. If there are persons working on the system whose access should be limited, the following risks should be considered:

- **Open system access.** This means there may be no control over who can either use the AIS or enter the computer room.
- **Theft of data.** Personal data maybe stolen from the computer room or other places where it is stored.
- **Unprotected files.** Personal data files may not be protected from unauthorized access by other users of the AIS. This applies to online files and also to offline files, such as files on magnetic tapes. The offline files are sometimes accessible simply by requesting a tape be mounted.
- **Dial-in access.** There is serious danger that unauthorized persons can access the system when remote, dial-in access is allowed.
- **Open access during abnormal circumstances.** Personal data that is adequately protected during normal operations may not be adequately protected under abnormal circumstances. Abnormal circumstances include power failures, bomb threats, and natural disasters, such as fire or flood.

The physical destruction or disabling of the AIS is not normally a primary risk to privacy. However, all computer systems presently in use are vulnerable to deliberate penetrations that can bypass security controls. These types of security penetrations require extensive technical knowledge. At present, the Navy has experienced very few of these deliberate penetrations. Commands designing large computer networks should consider the following risks early in the planning stage:

- **Misidentified access.** Passwords are often used to control access to a computer or to data, but they are notoriously easy to obtain if their use is not carefully controlled. Furthermore, a person may use an already logged-in terminal, which the authorized user has left unattended, or may capture a communications port as an authorized user attempts to disconnect from it.
- **Operating system flaws.** Design and implementation errors in operating systems allow a user to gain control of the system. once the user is in control, the auditing controls can be disabled, the audit trails erased, and any information on the system accessed.
- **Subverting programs.** Programs containing hidden subprograms that disable security protections can be submitted. Other programs can copy personal files into existing or misidentified files to use when protection is relaxed.
- **Spoofing.** Actions can be taken to mislead system personnel or the system software into performing an operation that appears normal but actually results in unauthorized access.
- **Eavesdropping.** Communications lines can be monitored by unauthorized terminals to obtain or modify information or to gain unauthorized access to an AIS.

INFORMATION MANAGEMENT PRACTICES

Information management practices refer to the techniques and procedures used to control the many operations performed on information to accomplish the command's objectives. They do not extend to the essential managerial determination of the need for and uses of information in relation to any command's mission. In this context, information management includes data collection, validation and transformation; information processing or handling; record keeping; information control, display, and presentation; and, finally, standardization of information management operations.

Before enacting new policies in personal data handling procedures, AIS technical managers should analyze current practices. To facilitate the explanation of their roles, the information management guidelines presented in the following material are grouped into major categories: handling of personal data, maintenance of records to trace the disposition of personal data, data processing practices, programming practices, assignment of responsibilities, and procedural inspecting. Every practice presented may not be required at every Navy AIS facility by upper management. Select only the suggested practices relevant to the designated command's environment and mission, or approved by upper management.

Handling of Personal Data

Access to personal information will be limited to authorized individuals of agencies in the Department of Defense who have an official need for the record, except when the information is otherwise releasable under the disclosure or access provisions of the Privacy Act.

The following practices are suggested for the handling of personal data:

- Prepare a procedures handbook. Describe the precautions to be used and obligations of computer facility personnel during the physical handling of all personal data. Include a reference regarding the applicability of the procedures to those government contractors who are subject to the Privacy Act. Personal information that is processed, accessed, maintained, or disposed of by contractors must be handled within the terms and conditions of Section 7-104.96 of the Defense Acquisition Regulation.
- Label all recording media that contain personal data. Labeling the media reduces the probability of accidental abuse of personal data. It also aids in fixing the blame in the event of negligent or willfully malicious abuse. If the information resides on removable storage media, it should be externally labeled. External warnings must clearly indicate that the media contain personal information subject to the Privacy Act; for example, PERSONAL DATA—PRIVACY ACT of 1974. Note that abbreviations must not be used.
- Store personal data in a manner that conditions users to respect its confidentiality. For example, store personal data under lock and key when not being used.
- If a program generates reports containing personal data, have the program print clear warnings of the presence of such data on the reports.
- Color code all computer tape reels, disk pack covers, and so on, which contain personal data, so they can be afforded the special protection required by law.
- Keep a record of all categories of personal data contained in computer-generated reports. This facilitates compliance with the requirements that each command identify all personal data files and their routine uses by the command.
- Carefully control products of intermediate processing steps. For example, control scratch tapes and disk packs to ensure they do not contribute to unauthorized disclosure of personal data.
- Maintain an up-to-date hard-copy authorization list. The list should include all individuals (computer personnel as well as system users) allowed to access personal data. It is used in access control and authorization validation.
- Maintain an up-to-date hard-copy data dictionary. This dictionary should be the complete inventory of personal data files within the computer facility to account for all obligations and risks.

Maintenance of Records to Trace the Disposition of Personal Data

The following practices are suggested for the maintenance of records:

- Establish procedures for maintaining correct, current accounting of all new personal data brought into the computer facility.
- Log each transfer of storage media containing personal data to or from the computer facility.
- Maintain logbooks for terminals used to access personal data by system users.

Data Processing Practices

The following practices are suggested for data processing procedures:

- Use control numbers to account for personal data upon receipt and during input, storage, and processing.
- Verify the accuracy of the personal data acquisition and entry methods employed.
- Take both regular and unscheduled inventories of all tape and disk storage media to ensure accurate accounting for all personal data.
- Use carefully devised backup procedures for personal data. A copy of the data should be kept at a second location if its maintenance is required by law.
- Create a records retention timetable covering all personal data and stating minimally the data

type, the retention period, and the authority responsible for making the retention decision.

- After a computer failure, check all personal data that was being processed at the time of failure for inaccuracies resulting from the failure.
- If the data volumes permit economic processing, some sensitive applications may use a dedicated processing period.
- Examine files created from files known to contain personal data to ensure they cannot be used to regenerate any personal data. A formal process must be established to determine and certify that such files are releasable in any given instance.
- In aggregating personal data, consider whether the consequentfile has been increased in value to a theft-attracting level.
- When manipulating aggregations and combinations of personal data, make it impossible to trace any information concerning an individual. Take steps so that no inference, deduction, or derivation processes can be used to recover personal data.

Programming Practices

The following practices are suggested for programming procedures:

- Subject all programming development and modification to independent checking by a second programmer, bound by procedural requirements developed by a responsible supervisor.
- Inventory current programs that process or access personal data; verify their authorized usage.
- Enforce programming practices that clearly and fully identify personal data in any computer program.
- Strictly control and require written authorization for all operating system changes that involve software security.

Assignment of Responsibilities

The following practices are suggested for the assignment of responsibilities:

- Designate an individual responsible for examining facility practices in the storage, use, and processing of personal data, including the use of security measures, information management practices, and computer system access controls. Both internal uses and the authorized external transfer of data should be considered by this individual and any risks reported to the relevant upper management authority and the AIS technical manager.
- Designate an individual responsible during each processing period (shift) for ensuring the facility is adequately staffed with competent personnel and enforcing the policies for the protection of personal data.
- Ensure that all military, civil service, and other employees engaged in the handling or processing of personal data adhere to established codes of conduct.

Procedural Inspecting

Whenever appropriate, conduct an independent examination of established procedures. Inspections of both specific information flow and general practices are possible. The following points should be considered when developing an inspection:

- Inspecting groups can be established within organizations to provide assurance of compliance independent of those directly responsible.
- Independent, outside inspectors can be contacted to provide similar assurance at irregular intervals.
- Inspection reports should be maintained for routine inspection and used to provide additional data for tracing compromises of confidentiality.

IDENTIFICATION TECHNIQUES

Once security measures and information management practices are established, the AIS technical manager should consider methods of personal identification of individuals for authorized access to the AIS facility. The identification of each individual allowed to use a system is a necessary step in safeguarding the data contained in that system.

For a broader knowledge of personal identification and identification techniques, refer to *Guidelines on*

Evaluation of Techniques for Automated Personal Identification, FIPS PUB 48.

SUMMARY

AIS security is everyone's job. The key word is *PROTECT:* take all reasonable measures to protect our AIS assets. Be sure you know what to do if a fire breaks out, the air conditioning goes off, the power goes down (with or without an UPS), or an unauthorized person is in your computer facility.

Learn the AIS terminology and requirements. Keep alert; early detection of problems is the key to minimizing damage and destruction.

Security of all types should be a continuous matter with every AIS technical manager. In this chapter, we have scratched only the surface of the material available on classified security, physical security, and security and privacy of data. It is a subject with which everyone should be completely up-todate. Study the material presented and referenced in this chapter to become knowledgeable in AIS security.

CHAPTER 5

GENERAL SECURITY

LEARNING OBJECTIVES

Upon completing this chapter, you should be able to do the following:

- *Identify the procedures for verifying the identification and clearance of recipients.*
- *Identify the procedures for TEMPEST requirements.*
- *Identify methods of controlling access to security areas, including designation of restricted areas, requirements relating to lock combinations, and procedures for sanitizing sites and equipment.*
- *Identify the procedures and regulations for marking material and conducting inventories of classified material (Secret and below).*
- *Identify the procedures used for clearing media and hardware of classified material (Secret and below).*
- *Identify the regulations and procedures for declassification or destruction of classified hardware and the destruction of classified material (Secret and below).*
- *Identify the regulations and procedures covering the receipt, inspection, handling, destruction, and verification of classified material (SPECAT or Top Secret and above).*

Your duties as a Radioman will require that you handle considerable amounts of classified information and equipment. You should be able to recognize classified matter and know what to do—or not do—with it. Security is as basic a part of your assignment as operating telecommunications equipment. Safeguarding classified information is an integral part of your everyday duties.

The security of the United States in general, and of naval operation in particular, depends upon the safeguarding of classified information. As a Radioman, you will learn information of vital importance to both the military and the nation. At times, vast amounts of classified message information will pass through your hands.

You must be security conscious to the point that you automatically exercise proper discretion in the discharge of your duties. In this way, security of classified information becomes a natural element of every task and not an additionally imposed burden.

RECIPIENT'S IDENTIFICATION AND CLEARANCE

Identification may be provided with the member military identification card, command identification cards or badges. Normally, local standard operating procedures cover the individual command's requirements. Guidelines for identification and access are contained in the *Department of the Navy Information and Personnel Security Program*

Regulation, OPNAVINST 5510.1, hereinafter called the *Security Manual.*

- Military identification cards are required to be carried by all active duty military. They aid only in recognizing the individual, not access or clearance.
- A command identification card/badge assists in identifying the level of security clearance of the holder or where the holder is authorized to enter. These cards/badges are only an aid and may not be used as the basis for granting access to information or areas.

A personnel security clearance will be issued to an individual by the Department of the Navy Central Adjudication Facility (DONCAF), or other designated clearance authority with favorable completion of required paperwork in accordance with the *Security Manual*. A copy of OPNAV 5510/413 (Clearance Report) will be filed in the member's permanent service record and in the security officer's files.

CONTROL OF COMPROMISING EMANATIONS (TEMPEST)

Compromising emanations (CE), referred to as "TEMPEST," are unintentional data-related or intelligence-bearing signals. If these signals are intercepted and analyzed, they could disclose the information transmitted, received, handled, or otherwise processed by electrical information-processing equipment or systems. Any electrical information-processing device, whether an ordinary electric typewriter or a large complex data processor, may emit compromising emanations.

TEMPEST VULNERABILITY ASSESSMENT (TVA)

The vulnerability of a ship, aircraft, shore station, transportable equipment, or a contractor facility is determined by a TEMPEST Vulnerability Assessment. This assessment includes each of the following factors, which, together, create vulnerability:

Susceptibility— The probability that TEMPEST signals exist and are open to exploitation.

Environment— The primary environmental considerations are the geographical location of a ship, aircraft, shore station, or contractor facility; physically and electrically controlled spaces; adherence to approved installation criteria; and the use of TEMPEST-approved equipment or systems.

- **Threat—** The capability and motivation of an enemy to exploit the TEMPEST signal.

The interaction of all of these factors determines the vulnerability. From this assessment and considering the category, classification, or sensitivity of the information involved, a determination will be made. An Instrumented TEMPEST Survey (ITS) will be scheduled, or the requestor will be placed in the "acceptable risk" category.

Tempest Vulnerability Assessment Request (TVAR)

A TVAR must be submitted prior to processing classified data. This request should be sent to the Naval Criminal Investigative Service, Washington D.C., with a copy to CO, NAVELEXSECCEN and other commands as appropriate. The list of required information is available in *Navy Implementation of National Policy on Control of Compromising Emanations (U)*, OPNAVINST C5510.93.

Some ships are identified by CNO as high TEMPEST risk platforms. Those which are likely to be the target of hostile TEMPEST collection efforts will be scheduled for an Instrumented TEMPEST Survey (ITS). No TVAR is required from any ship.

EMISSION CONTROL (EMCON)

EMCON is used to prevent an enemy from detecting, identifying, and locating friendly forces. It is also used to minimize electromagnetic interference among friendly systems. EMCON is normally imposed by a commander to control all electromagnetic radiations. Once EMCON is imposed, general or specific restrictions may be added to the EMCON order, depending on the operational, intelligence, or technical factors for the area affected.

For radiomen, EMCON usually means either full radio silence or HF EMCON. The most secure communications methods during EMCON reduce, but do not eliminate, the possibility of identification. It is assumed that any electromagnetic radiation will be immediately detected, and the position of the transmitting ship will be fixed by an enemy. You will find detailed information on the implementation of EMCON and its degree of adjustment in *Electronic*

Warfare Coordination, NWP 3-51.1 (formerly NWP 10-1-40).

SECURITY AREAS

Different spaces aboard ship and different areas within a shore activity usually have varying degrees of security importance. The degree of security of each area depends upon its purpose and the nature of the work, information, equipment, or materials concerned. Access to security areas must be controlled in a manner consistent with the security level.

SANITIZING SITE AND EQUIPMENT

Sanitizing an area or equipment is done to make it acceptable for access by personnel who are not cleared. This is used to prevent unauthorized persons from gaining access that would allow them to identify the purpose or nature of your work, information, equipment and materials concerned.

To meet this situation, each command should apply differing protective measures commensurate with the degree of security importance. Persons who have not been cleared for access to the information contained within the area, with appropriate approval, may be admitted into an area, but they must be controlled by an escort at all times. Follow guidelines set forth in the *Security Manual* and local standard operating procedures.

A few of the basic requirements are listed below.

- Remove, turn over, or place in drawers any classified material that may be out on desks.
- Replace any keying material in the safe and lock.
- Cover any status boards showing conditions of equipment, frequencies, systems, and so forth.
- Cover all frequencies dialed into equipment.
- Cover monitors or turn off monitor screens if possible.
- Do not conduct any work-related discussions.

At no time will the escort leave someone unattended. The watch section or day working staff maybe required to support the escort in cases where work is being conducted by numerous uncleared personnel in more than one area.

RESTRICTED AREAS

Designating security spaces as restricted areas provides an effective and efficient means for a command to restrict access and control movement. In restricted areas, only those personnel whose duties actually require access and who have been granted appropriate security clearance are allowed freedom of movement within the area.

Persons who have not been cleared for access to the information contained within the area may, with appropriate approval, be admitted into the area. While in these spaces, however, uncleared persons must be escorted, or other security procedures implemented to prevent any unauthorized disclosure of classified information.

All designated restricted areas must have warning signs posted at all entrances and exits. These areas must have clearly defined perimeters and, if appropriate, Restricted Area warning signs posted on fences and barriers.

Access to Spaces

The commanding officer or the officer in charge over security spaces is responsible for controlling access to these areas. Procedures should limit access to security spaces only to those persons who have a need to know. No one has a right to have access to classified information or spaces based solely on clearance, rank, or position.

Each command establishes a pass or badge identification system to restrict access and to help control movement. Control of movement within the area is normally accomplished by requiring the display or presentation of the pass or badge for that particular area.

Access List

Admission of visitors to communications spaces is a topic of major concern to radiomen since access to communications spaces under operating conditions usually permits viewing of classified traffic and equipment. A security badge does not automatically mean that visitors have a “need to know” or that they should be granted access. Admission to communications spaces is granted only to personnel whose names, rates/ranks, and clearance level appear on the official access list.

Access lists, which must be signed and approved by the commanding officer, should be posted at each entrance to a communications space. Admission of persons other than those on the access list is subject to the specific approval of the commanding officer or his or her designated representative.

Personnel not on the access list nor specifically granted permission by the commanding officer for entry must be escorted or supervised at all times while in communications spaces.

Communications Center Visitors Log

A communications center visitors log (or register) is used to record the arrival and departure of authorized personnel whose names do not appear on the access list. *Fleet Communications* (U), NTP 4, recommends the following column headings for visitors logs:

- Date;
- Visitor's printed name;
- Organization the visitor is representing;
- Purpose of visit;
- Visitor's signature;
- Officer authorizing access to restricted area(s);
- Escort's name;
- Time in; and
- Time out.

Access to Classified NATO Messages

Only those personnel who hold a security clearance equal to or greater than the clearance required for U.S. material may have access to NATO messages. NATO messages and documents belong to NATO and must not be passed outside the NATO organization. *NATO Security Procedures (U)*, OPNAVINST C5510.101, is the authority for the proper handling, storage, accounting, classification, and clearances of NATO material.

The final responsibility for determining whether a person is granted access to a security area rests upon the individual who has the authorized possession, knowledge, or control of the information involved and not upon the prospective recipient. No number of written rules or governing statutes can replace individual initiative and common sense. As we mentioned earlier, no one has a right to access based solely upon security clearance, rank, or position.

STORAGE OF CLASSIFIED MATERIAL

All classified matter not in actual use must be stored in a manner that will guarantee its protection. The degree of protection necessary depends on the classification category, quantity, and scope of the material involved. Normally, the type and extent of physical protection required are determined before an activity begins its day-to-day or watch-to-watch routine.

It is very likely that an appropriate physical security program is already in effect when you report aboard. Details concerning physical security standards and requirements for classified information are contained in the *Security Manual.*

Unattended Containers

If you find an open and unattended container or cabinet containing classified matter, you should report it to the senior duty officer. Do not touch the container or contents, but guard them until the duty officer arrives. The duty officer then assumes responsibility for such further actions as locking the security container, recalling the responsible person or persons, and reporting the security violation to the commanding officer. The custodian must conduct an immediate inventory of the contents of the security container and report any loss to the commanding officer.

Combinations

Combinations to security containers containing classified material are made available only to those persons whose duties require access to them. The combinations of security containers containing classified information must be changed at least every 2 years, unless more frequent change is dictated by the type of material stored within. Combinations must also be changed under the following circumstances:

- When an individual knowing the combination no longer requires access;
- When the combination has been subject to possible compromise or the security container has been discovered unlocked and unattended; and
- When the container is taken out of service.

The combination of a security container used for the storage of classified material is assigned a security classification equal to the highest category of classified material authorized to be stored in the container. Records of combinations are sealed in an envelope (Standard Form 700) and kept on file in a central location designated by the commanding officer.

Cipher Locks

Cipher locks and safe combinations are handled in accordance with guidelines found in the *Security Manual*. With the addition of electrically actuated locks (that is, cipher and magnetic strip card locks), this type of lock still does not afford the degree of protection required for classified information. They may NOT be used as the primary means to safeguard classified material. Cipher or magnetic strip card locks are normally used for access to an area only.

GENERAL MARKING REQUIREMENTS

Classified documents and material must be clearly and conspicuously marked. Special markings, such as LIMDIS and Restricted Data, are normally placed near the classification markings. These markings inform and warn recipients of the classification assigned and indicate the level of protection required. These markings also identify the information that must be withheld from unauthorized persons.

Top Secret, Secret, and Confidential classification markings must be stamped, printed, or written in capital letters larger than those used in the text of the document. These security markings should be red in color, when practicable, and be placed at the top and bottom center of each page.

All reproductions or copies of classified materials, regardless of form, must bear clearly legible security classification markings and notations in the same manner as on the copied or reproduced material. Copying equipment does not always clearly reproduce all colors of ink or marginal images. If the reproduction process does not clearly reproduce the security markings appearing on the original copy, all copies must be marked in the same positions and size as on the original.

Paragraph markings are required for classified documents. The appropriate security markings are placed at the beginning of the classified paragraph. The symbols used to indicate paragraph classification are (TS) for Top Secret,(S) for Secret, (C)for Confidential, and (U) for Unclassified.

It is not uncommon to see foreign-originated classified information in U.S. messages and documents. Paragraphs that contain foreign-originated classified information must be properly marked; for example, "U.K.(C)" or "NATO(S)."

At the beginning of Restricted Data and Formerly Restricted Data paragraphs, use the appropriate classification symbol with the abbreviation "RD" or "FRD," such as "(S-RD)," "(C-FRD)."

Titles and subjects are classified according to their content, regardless of the overall classification of the document. Normally, the symbols indicating the classification assigned to a title or subject are placed in parentheses immediately following the item, as in the following example:

Subj: BASIC OPERATIONAL COMMUNICATIONS DOCTRINE (U)

SPECIAL-HANDLING MARKINGS

In addition to security classification categories, other markings also appear on some documents and messages. Among these markings are such designations as Restricted Data (RD), Formerly Restricted Data (FRD), LIMDIS, FOUO, EFTO, SPECAT, PERSONAL FOR, NATO RESTRICTED, and ALLIED RESTRICTED.

Restricted Data and Formerly Restricted Data

The marking "Restricted Data" (RD) is applied to all data concerned with the design, manufacture, or use of nuclear weapons. Also included in this category is the special nuclear material used in energy production.

The marking "Formerly Restricted Data" (FRD) pertains to defense information that has been removed from the RD category but must still be safeguarded as classified defense information. FRD material cannot be released to foreign nationals except under specific international agreement.

LIMDIS (Limited Distribution)

The LIMDIS designator is applied only to classified messages which, because of the subject matter, require limited distribution within the addressed activity.

For Official Use Only (FOUO)

FOUO is the designation used on official information not requiring a security classification but which must be withheld and protected from public release. Unclassified messages containing FOUO information must have the abbreviation "FOUO" after the designation "UNCLAS."

Encrypt for Transmission Only (EFTO)

Certain categories of unclassified messages maybe identified as having potential value if subject to analysis, but do not meet the criteria for security classification. The special designation "EFTO" was established to protect these unclassified messages during electrical transmission.

EFTO is not required on unclassified messages addressed exclusively among Navy, Marine Corps, and Coast Guard commands. EFTO is authorized for use within the Department of Defense, including the National Security Agency. However, EFTO is required on FOUO messages addressed to DOD activities outside the continental United States. Bear in mind, however, that just because information is FOUO, it is not automatically EFTO, and vice versa.

As we mentioned earlier, EFTO is a transmission marking for unclassified messages. FOUO markings, however, define a certain category of information requiring special handling. Neither FOUO nor EFTO markings are security classifications; both are special-handling designations. You can find detailed information on EFTO and FOUO markings in *Basic Operational Communications Doctrine (U)*, NWP 4.

SPECAT

The SPECAT marking means special category. SPECAT messages are classified messages identified with a special project or subject. SPECAT messages require special-handling procedures in addition to the handling procedures for the security classification of the message. There are four SPECAT categories:

- SPECAT;
- SPECAT EXCLUSIVE FOR (SEF);
- SPECAT Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI); and
- PSEUDO-SPECAT.

SPECAT and SPECAT EXCLUSIVE FOR messages must be at least Confidential. SPECAT SIOP-ESI messages are always Top Secret. PSEUDO-SPECAT messages are normally unclassified messages that require limited distribution. Examples of PSEUDO-SPECAT messages include AMCROSS messages, urinalysis test results, and HIV test results.

SPECAT messages are handled only by those personnel who are authorized by the commanding officer in writing to view them. The types of information assigned SPECAT and handling procedures can be found in NWP 4 and in *Fleet Communications (U)*, NWP 4, respectively.

PERSONAL FOR

PERSONAL FOR is the marking applied when message distribution must be limited to the named recipient. Only flag officers, officers in a command status, or their designated representatives may originate PERSONAL FOR messages.

NATO RESTRICTED

The United States does not have a security classification equivalent to NATO RESTRICTED. NATO messages classified as restricted must be safeguarded in a manner similar to that for FOUO messages. Messages originated by NATO must be handled in accordance with *NATO Security Procedures (U)*, OPNAVINST C5510.101.

ALLIED RESTRICTED

The United States does not have a security classification equivalent to ALLIED RESTRICTED. However, these messages must be handled in the same manner as Confidential messages. U.S.-originated messages containing ALLIED RESTRICTED information are marked as "Confidential" immediately following the security classification.

The *Security Manual* contains complete information on paragraph, subparagraph, and document markings.

HANDLING AND STORAGE OF CLASSIFIED MATERIAL

Classified messages must be provided accounting and control procedures that correspond to their assigned classification. Accounting and control of classified messages serve the following functions:

- Limit dissemination;
- Prevent unnecessary reproduction; and
- Determine the office or person normally responsible for the security of the material.

With Top Secret messages, it is also important to keep a current record of who has the information and who has seen it.

Since distinctions are made among the three levels of classification, distinctions are also made in the degree of accountability and control. Within each command, specific control and accountability procedures are established to ensure that classified material is properly controlled and that access is limited only to cleared personnel.

SECURITY PERSONNEL

To control classified information with maximum efficiency, the commanding officer designates a security manager, usually an officer. The security manager is responsible for the command's overall security program, which includes the security of classified information, personnel security, and the command's security education program.

In addition, the commanding officer usually appoints a Top Secret Control Officer (TSCO). The TSCO is responsible for the receipt, custody, accounting, and disposition of Top Secret material in the command. The TSCO is normally subordinate to the security manager. If a separate person is not designated as the TSCO, the security manager maybe designated as TSCO. The duties of the security manager and the TSCO are outlined in the *Security Manual.*

Besides the security manager and the TSCO, every command involved in processing data in an automated system must designate an Information System Security Officer (ISSO). The ISSO is responsible to the security manager for the protection of classified information processed in the automated system.

Custody of Classified Material

An individual who has possession of or is charged with the responsibility for safeguarding and accounting for classified material or information is the "custodian" of that material or information. As a Radioman, you are constantly in possession of classified material, including messages, publications, and equipment. Therefore, you are a custodian of classified material as long as the material is in your possession.

As custodian of classified material, you are responsible for protecting and accounting for the material at all times. You must ensure that the material is protected from disclosure to uncleared personnel, such as a visitor being escorted through your working spaces. If working outside of normal communication spaces, you must ensure that classified material is locked in an approved security container when the material is not in use or under direct supervision.

CARE DURING WORKING HOURS.— Every Radioman must take the necessary precautions to prevent access to classified information by unauthorized persons. These precautions include:

- When removed from storage for working purposes, classified documents must be kept under constant surveillance or face down or covered when not in use.
- Preliminary drafts, carbon sheets, plates, stencils, notes, work sheets, and all similar items containing classified information require special precautions. They must be either destroyed immediately after they have served their purpose or given the same classification and safeguarded in the same manner as the classified material produced from them.
- Typewriter ribbons used in typing classified material must be protected in the same manner as the highest level of classification for which they have been used. Fabric typewriter ribbons may be considered as unclassified when both the upper and lower sections have been recycled through the machine five times in the course of regular typing. Those ribbons that are classified must be destroyed as classified waste.

CARE AFTER WORKING HOURS.— At the close of each watch or working day, all classified material that is passed from watch to watch must be properly inventoried. Custody is then transferred to the relieving watch supervisor. All other classified material must be locked in an approved security container. A system of security checks at the close of each working day is the best method to ensure that all classified material held is properly protected. Whether your watch section is being relieved by the oncoming watch or you are securing an office space, you should make an inspection to ensure as a minimum that:

- All classified material is properly stored.
- Burn bags are properly stored or destroyed.

- Wastebaskets do not contain classified material.
- Classified notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts, and similar papers have been properly stored or destroyed. As a matter of routine, such items should be placed in burn bags immediately after they have served their purpose.
- When classified material is secured in security containers, the dial of combination locks should be rotated at least four complete turns in the same direction.

CLASSIFIED MATERIAL (SPECAT/TS AND ABOVE)

Classified material excludes communications security (COMSEC) material, which is handled by CMS 1 procedures. Further in-depth information on classified material can be found in the *Security Manual* and in NTP 4.

1. Receive:

The Top Secret Control Officer (TSCO) is responsible for receiving, maintaining "cradle to grave" accountability registers for, distributing and destroying Top Secret, SPECAT/TS, and above documents.

All Top Secret, SPECAT/TS, and above material received or originated by a command, which the TSCO is responsible for, is entered into the command's accountability log.

Top Secret, SPECAT/TS, and above message traffic, handled by naval communication stations for relay or broadcast delivery only, or received by an afloat command via the fleet broadcast but not addressed to that command will be accounted for and destroyed in accordance with NTP 4.

Top Secret, SPECAT/TS, and above messages addressed to the command are:

- Logged into the cryptocenter log.
- Master copy is placed in the cryptocenter file, and fillers are placed in the appropriate files.
- One copy is given to the TSCO for entry into the command's controlled distribution register.

Top Secret, SPECAT/TS, and above messages received by an afloat command but NOT addressed to the command via the broadcast:

- Only the text will be removed from the monitor roll.
- The message will be destroyed, and the monitor roll will be initialed by two witnessing officials.
- The broadcast serial number checkoff sheet will also be initialed by two witnessing officials.

2. Destroy:

Top Secret, SPECAT/TS, and above material will be destroyed by two witnessing officials. Persons performing any destruction must have a clearance level equal to or higher than the material being destroyed. The destruction of Top Secret, SPECAT/TS, and above material must be recorded. Destruction may be recorded on OPNAV form 5511/12 (figure 5-1), or any other record which includes complete identification of the material, number of copies destroyed, date of destruction, and personnel completing destruction. The two witnessing officials responsible for the destruction must sign the record of destruction. The records of the destruction are retained for 2 years.

3. Verify destruction:

The destruction of Top Secret, SPECAT/TS, and above material must be verified by both witnesses signing the destruction sheet and either turning it over to the TSCO or placing it in the cryptocenter master file until it is superseded, usually within 2 years.

HANDLING TOP SECRET MATERIAL

Although administrative records are maintained for each classification category, the strictest control system is required for Top Secret material.

Except for publications containing a distribution list by copy number, all Top Secret documents and each item of Top Secret equipment must be serially numbered at the time of origination. Also, each document must be marked to indicate its copy number (for example, Copy No. ___ of ___ Copies).

Each page of a Top Secret document not containing a list of effective pages (LOEP) must be individually numbered (for example, Page ___ of ___ pages). Top Secret documents are required to have a list of effective pages and a page-check page. Top Secret documents may be reproduced only with the permission of the originator or higher authority.

CLASSIFIED MATERIAL DESTRUCTION REPORT OPNAV 5511/12 (REV. 3-75) S/N 0107-LF-055-1160 TO: Commanding Officer, USS NEVERSAIL	CLASSIFICATION *(Indicate when title or other identification is classified)* UNCLASSIFIED

FROM *(Name and address of activity)*
Top Secret Control Officer

The classified material described below has been destroyed in accordance with regulations established by the Department of the Navy Information Security Program Regulation; OPNAV INSTRUCTION 5510.1G.

The purpose of this form is to provide activities with a record of destruction of classified material. Also, copies may be utilized for reports to activities originating material, where such reports are necessary.

DESCRIPTION OF MATERIAL

SERIAL/DTG	ORIGINATOR	DATE	COPY NO.	LOG/ ROUTE SHEET NO.	ENCLOSURES (IDENT. & NO.)	TOTAL NO. PAGES
00052	CINCPACFLT letter	(Date)	1	4		4

OFFICER OR INDIVIDUAL AUTHORIZING DESTRUCTION *(Signature, Rank/Rate/Grade)*	DATE OF DESTRUCTION (Date)
WITNESSING OFFICIAL *(Signature, Rank/Rate/Grade)* John Doe	WITNESSING OFFICIAL *(Signature, Rank/Rate/Grade)* Jane Smith

Figure 5-1.—Classified Material Destruction Report.

A continuous chain of receipts for Top Secret material must be maintained. Moreover, a Record of Disclosure, OPNAV form 5511/13, for Top Secret material is attached to each document that circulates within a command or activity. Each person having knowledge of the contents of a Top Secret document must sign the attached Record of Disclosure. Top Secret messages, documents, and publications must be stored in a security container separate from those classified Secret and below.

HANDLING SECRET MATERIAL

Every command is required to establish administrative procedures for recording all Secret material originated and received. These administrative procedures, as a minimum, must include a system of accountability for Secret matter distributed or routed within the command, such as a communications log. Accounting of Secret material may or may not be centralized.

Unlike Top Secret material, Secret material does not require signed receipts distributed or routed within the command. However, it is extremely important that you ensure that the person who is receiving Secret messages or material is properly cleared, and his or her name appears on an access list released by the commanding officer.

HANDLING CONFIDENTIAL MATERIAL

Procedures for handling Confidential material are less stringent than those for Secret. There is no requirement to maintain records of receipt, distribution, or disposition of Confidential material. However, Confidential material must still be protected from unauthorized disclosure by access control and compliance with regulations on marking, storage, transmission, and destruction.

HANDLING CLASSIFIED AIS MATERIAL

Classified AIS storage media and output must be controlled and safeguarded in accordance with its security classification. Specific procedures on security requirements for handling and storing AIS material are found in the *Department of the Navy Automatic Data Processing Security Program*, OPNAVINST 5239.1.

CLEARING MEDIA AND HARDWARE

Declassifying AIS media is a procedure to erase totally all classified information stored in the media. The clearing of AIS media is used to erase classified information that lacks the totality and finality of declassifying. There are distinct and specific techniques to clear media and hardware; a sampling follows:

- Magnetic tapes: Overwrite one item with any one character or perform degaussing.
- Magnetic media used to store analog, video, or other nondigital information: Overwrite using analog signals instead of digital.
- Internal memory, buffers, registers, or similar storage areas: Use hardware clear switch, power on reset cycle or a program designed to overwrite the storage area.
- Cathode-ray tubes (CRTs): Ensure that there is no burned-in classified information by inspecting the screen surface.

DESTRUCTION OF CLASSIFIED MATERIAL

Classified material that is no longer required should not be allowed to accumulate. Destruction of superseded and obsolete classified materials that have served their purpose is termed "routine destruction."

ROUTINE DESTRUCTION

There are specific directives that authorize the routine destruction of publications, message files, and cryptomaterials. As a Radioman, you should carefully study these directives so that you may properly comply with them. Additionally, the letter of promulgation of publications often sets forth disposition instructions about destruction requirements for that publication. Other materials, such as classified rough drafts, worksheets, and similar items, are periodically destroyed to prevent their accumulation.

Top Secret, Secret, and Confidential material may be destroyed by burning, pulping, pulverizing, or shredding. Destruction must be complete and reconstruction of material impossible. The most efficient method of destroying combustible material is by burning.

DESTRUCTION PROCEDURES AND REPORTS

Top Secret material will be destroyed by two witnessing officials. Persons performing any destruction must have a clearance level equal to or

higher than the material being destroyed. Destruction will be recorded on a record that provides for complete identification of the material being destroyed. Destruction records must include number of copies destroyed, date of destruction, and personnel completing destruction. These records are maintained for 2 years.

Secret messages must be destroyed following the two-person rule, without a record of destruction. Alternatively, one person may destroy Secret messages if a record of destruction is made. The commanding officer may impose additional controls for Secret messages if warranted and if they reasonably balance security against operational efficiency.

Confidential material and classified waste are destroyed by authorized means. Personnel performing destruction must hold an appropriate clearance and are not required to record destruction.

If the material has been placed in burn bags for central disposal, the destruction record is signed by the witnessing officials at the time the material is placed in the burn bags. Records of destruction must be retained for 2 years.

All burn bags must be given the same protection as the highest classification of material in them until they are destroyed. Since several burn bags may accumulate for burning, it is important to keep an accurate record of the number of bags to be burned. Burn bags must be serially numbered and a record kept of all subsequent handling until destroyed.

Burning

As a Radioman, you will probably assist in the burning of classified material. Every member of a burn detail must know exactly what is to be burned and should double-check burn material against an inventory list before the material is burned.

To provide for accountability of the burn bags, the supervisor of a burn detail must be sure that the bags are numbered (or counted) before they are removed from the workspaces. The supervisor of a burn detail must have either a log or checkoff list that lists the number of bags to be burned. At the destruction site, each bag is checked off the list as it is destroyed in the presence of the witnessing officials. Witnessing officials are persons performing any destruction. They must have a clearance equal to or higher than the material being destroyed.

To ensure the complete destruction of bound publications, the pages must be torn apart and crumpled before they are placed in bags. All material must be watched until it is completely consumed. The ashes must be broken up and scattered so that no scraps escape destruction.

Shredding

Crosscut shredding machines are relatively quiet and may be used aboard ships where incinerator facilities are not available. Crosscut shredders are replacing incinerators in many areas where burning is not allowed because of the Clean Air Act. Crosscut shredding machines must reduce classified material to shreds no greater than 3/64 inch wide by 1/2 inch long. Crosscut shredding suffices as complete destruction of classified material, and the residue may be handled as unclassified material with the exception of some COMSEC material. Not all crosscut shredders are suitable for destroying microfiche, so make sure the one you are using has that capability before attempting to shred microfiche.

Pulverizing and Disintegrating

Pulverizers and disintegrators designed for destroying classified material are usually too noisy and dusty for office use unless installed in a noise- and dust-proof enclosure. Some pulverizers and disintegrators are designed to destroy paper products only. Others are designed to destroy film, typewriter ribbons, photographs, and other material.

Jettisoning or Sinking

Material to be jettisoned during emergency destruction must be placed in weighted bags. The sea depth should be 1,000 fathoms or more. However, if water depth is less than 1,000 fathoms, the material should still be jettisoned to prevent easy recovery.

EMERGENCY PLANS

Emergency plans provide for the protection, removal, or destruction of classified material. Commands holding classified material must develop an emergency plan to fit their needs. The primary requirement of an emergency plan is that it adequately provide for the rapid and complete destruction of the classified material. Emergency plans must cover three areas of emergencies:

- Natural disasters, such as hurricanes;
- Civil disturbances, such as rioting; and
- Enemy action.

Emergency plans should provide for the protection of classified material in such a manner as to minimize the risk of loss of life or injury to personnel.

For destruction, the command's emergency plan must do the following:

- Emphasize procedures and methods of destruction, including place and destruction equipment required;
- Clearly identify the exact location of all classified material;
- Prioritize material for destruction; and
- Assign personnel by billet, areas of responsibility for destruction.

Priorities

When the emergency plan is implemented, priority of destruction is based on the potential effect on national security should the material fall into hostile hands. COMSEC material is destroyed first. The priorities for emergency destruction are as follows:

- **FIRST PRIORITY—** Top Secret COMSEC material and classified components of equipment and all other Top Secret material;
- **SECOND PRIORITY—** Secret COMSEC material and all other Secret material;
- **THIRD PRIORITY—** Confidential COMSEC material and all other Confidential material.

After you have destroyed the classified for which you are responsible, you should destroy any unclassified equipment that could be of use to an enemy. You should also destroy pertinent technical, descriptive, and operating instructions.

FIRE PLANS

In addition to an emergency plan, a plan of action in the event of fire is also required. As with an emergency plan, it is important that all comunications personnel familiarize themselves with their command fire plan. Normally, the fire plan provides for the following:

- Local fire-fighting apparatus and personnel to operate the equipment;
- Evacuation of the area, including a decision whether to store classified material or remove it from the area; and
- Admitting outside fire fighters into the area.

PRECAUTIONARY ACTIONS

Precautionary destruction reduces the amount of classified material on hand in case emergency destruction later becomes necessary. Destruction priorities remain the same during precautionary destruction. However, when precautionary destruction is held, material essential to communications must not be destroyed. For example, communications operating procedures and publications that are to become effective in the near future would not be destroyed. Communications operating procedures that are already effective, necessary, and being used would also not be destroyed.

The following actions should be taken daily:

- All superseded material should be destroyed in accordance with its prescribed time frame.
- Unneeded material should be returned to the issuing agencies.
- Material should be stored in such a way as to make it readily accessible for removal during destruction.

Contrary to widespread opinion, there is no security policy requiring destruction of unclassified messages. However, some message centers with high volumes of classified and unclassified message traffic may find it more efficient to destroy all messages and intermingled files as though they were classified. Under some circumstances, units operating in foreign ports or waters and commands situated in foreign countries may take additional precautions in disposing of unclassified material.

SUMMARY

This chapter has discussed general security considerations to provide you with a working knowledge of this important aspect of your job. As a Radioman, you have a two-fold job concerning security. The first, of course, is to properly perform your duties within general security guidelines. Security guidelines pertain to everyone in every official capacity. Second, you must also perform your duties in such a manner as to protect the integrity and overall value of secure communications.

Security should be second nature insofar as the practice of personal habits is concerned. However, second nature does not mean "without thinking." It behooves all of us to take security seriously and practice sound security habits in the interests of naval operations and our overall national security.

Security precautions mentioned in this chapter do not guarantee complete protection nor do they attempt to meet every conceivable situation. Anyone who adopts a commonsense outlook can, however, solve most security problems and gain a knowledge of basic security regulations.

APPENDIX I

GLOSSARY

A

ADDRESS GROUPS— Four-letter groups assigned to represent a command, activity, or unit; used in the same manner as a call sign.

AIS FACILITY-RELATED INFORMATION— Workload, anticipated resource changes, number of operators available, the system capabilities, etc.

B

BACKLOG— The work waiting to be run (processed) on a computer.

BATCH PROCESSING— A method of processing in which similar items are grouped together and processed all at one time.

BOOK MESSAGE— A message for two or more addressees in which the drafter considers it unnecessary that each addressee be informed of the other(s).

C

CMS ALTERNATE CUSTODIAN— Responsible to the CMS custodian and commanding officer for the CMS account; is held accountable on the same level as the custodian.

CMS CUSTODIAN— Responsible to the commanding officer for the correct accountability and maintenance of the CMS account.

CMS LOCAL HOLDER— A command or activity that receives COMSEC material support from a CMS account command.

CMS USER— An individual CMS user that requires COMSEC material to accomplish an assigned duty, advancement study, or training purpose.

COMMUNICATIONS CENTER SUPERVISOR— Responsible for message processing, circuit operations, and supervision of personnel; responsible to the SWS, when assigned.

COMMSHIFT— A message sent to a NCTAMS to move its guard from one broadcast or servicing communications center to another.

COMMSPOT— A report to advise of any situation that might cause significant disruption to tactical communications.

COMNAVCOMTELCOM (COMMANDER, NAVAL COMPUTER AND TELECOMMUNICATIONSCOMMAND)— Headquarters for all naval shore-based communications.

CONTINGENCY PLANS— Backup plans for the continuation of an activity's mission during abnormal operating conditions.

CWO (COMMUNICATIONS WATCH OFFICER)— Responsible for the efficient running of the watch, including equipment and personnel; responsible to the communications officer.

D

DRAFTER— The person who actually composes a message for transmission.

DTG (DATE-TIME GROUP)— A method of assigning a date and time to message traffic consisting of six digits, two each to represent date, hour, and minutes; begins at the start of each new day at 0001Z.

E

EA (ELECTRONIC ATTACK)— Involves actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum. EA replaces electronic countermeasures (ECM).

ELECTROMAGNETIC SPECTRUM– The natural vibrations that occur when a force is applied to a substance. These vibrations occur with various speeds and intensities. The speed at which they occur is called frequency, and the distance between each vibration is called wavelength.

EMERGENCY PLAN— Provides for the protection, removal, or destruction of classified material.

EP (ELECTRONIC PROTECTION)— Involves actions taken to ensure friendly effective use of the electromagnetic spectrum despite an enemy's use of electronic warfare. EP replaces electronic counter-countermeasures (ECCM).

EXTRACTS— Portions of naval warfare publications that are extracted/reproduced for use in training or operations. All extracts must be properly marked with security classification and safeguarded.

F

FLASH PRECEDENCE— Identified by the precedence prosign "Z." Category reserved for initial enemy contact reports or operational combat messages of extreme urgency. Brevity is mandatory. Speed of service objective is not fixed. Handled as fast as humanly possible with an objective of less than 10 minutes.

FRD (FORMERLY RESTRICTED DATA)– Pertains to defense information that has been removed from the Restricted Data category but is still safeguarded as classified defense information.

G

GENERAL MESSAGE— A message with wide, predetermined and standard distribution.

I

IFF (IDENTIFICATION FRIEND OR FOE)— A system using electromagnetic transmissions to which equipment carried by friendly forces automatically responds to distinguish themselves from enemy forces.

IMMEDIATE PRECEDENCE— Identified by the precedence prosign "O." Delivery time reserved for very urgent messages relating to situations that gravely affect the security of national/allied forces. Examples of use: amplifying report of initial enemy contact or unusual major movements of military forces. Speed of service objective is 30 minutes to 1 hour.

INMARSAT (INTERNATIONAL MARITIME SATELLITE COMMUNICATIONS)— A satellite system that interfaces naval communications for the DON and commercial telecommunications authorized by law.

I/O CONTROL CLERK— The person responsible for the quality and control of data processing input and output media and products.

J

JETTISONING— A type of destruction that is completed by throwing material overboard at sea at a depth of at least 1,000 fathoms or more; also known as Sinking.

JOB DEPENDENCY— When a job requires the output from another job, it is said to be dependent on another job.

JOB-RELATED INFORMATION— Information about the resources, media, and time needed for a particular job.

JULIAN DATE— Consists of seven digits; the first three digits represent the date, and the last four digits represent the hour and minutes; begins on the first day of the calendar year.

M

MARS (MILITARY AFFILIATE RADIO SYSTEM)— Provides auxiliary communications to military, civil, and/or disaster officials during periods of emergency. Users are licensed by the Federal Communications Commission (FCC).

MULTIPLE-ADDRESS MESSAGE— A message with two or more addressees.

MULTIPROCESSING— A computer processing mode that provides for simultaneous processing of two or more programs or routines by use of multiple CPU's.

MULTIPROGRAMMING— A computer processing mode that provides for overlapping or interleaving the execution of two or more programs at the same time by a single processor.

N

NETWORKING— A processing mode that allows separate computers, joined by transmission lines, to share a group of common peripherals.

NWPL CLERK— Usually assigned by the NWPL custodian and is responsible for the upkeep and maintenance of the NWPL.

NWPL CUSTODIAN— Is responsible for managing the NWPL, usually assigned to an officer or senior petty officer as a collateral duty.

O

ONLINE— A method of data processing that allows users the ability to interact with the computer.

ORIGINATOR— The authority in whose name a message is sent.

P

PERSONAL FOR– Messages distributed to a single recipient. Only flag officers, officers in a command status, or their designated representative may originate PERSONAL FOR messages.

PLANNING PHASE— The initial scheduling phase in which information is gathered from the users.

POSTCOMPUTER PROCESSING— Ensuring output products are complete, accurate, and delivered to the user.

PRECAUTIONARY ACTIONS OR PRECAUTIONARY DESTRUCTION— An action to remove or reduce the amount of classified material on hand in case emergency destruction becomes necessary at a later time.

PRECEDENCE— A delivery time assigned to a message according to the urgency of that message, based solely on writer-to-reader time.

PRECOMPUTER PROCESSING— Ensuring all inputs are received on time.

PRIORITY PRECEDENCE— Identified by the precedence prosign "P." Delivery time reserved to message for essential information for the conduct of operations in progress. Examples of use: situation reports on position of front where attack is imminent, orders to aircraft formation or units to coincide with ground or naval operations. Speed of service objective is 1 to 6 hours.

R

RD (RESTRICTED DATA)— Pertains to all data concerned with the design, manufacture, or use of nuclear weapons or special nuclear material used in energy production.

REAL-TIME PROCESSING— A computer processing method in which data about a particular event is entered directly into the computer as the event occurs and is immediately processed so it can influence future processing.

RELEASER— A properly designated individual authorized to release messages for transmission in the name of the command or activity.

RESTRICTED AREA— Designated spaces that restrict access and control movement within.

ROUTINE PRECEDENCE— Identified by the precedence prosign "R." Delivery time assigned to be used for all types of message which does not justify a higher precedence. Examples of use: administrative, logistics, or personnel matters. Speed of service objective is 3 hours or start of business the following day.

S

SANITIZING— Makes an area or equipment acceptable for access by personnel who are not cleared.

SCHEDULER— The person responsible for preparing, distributing, and maintaining production schedules.

SCHEDULING— The interface between the user, I/O control, and computer operations.

SHREDDING— A type of destruction that involves using a cross-cut shredding machine. Residue must be reduced to shreds no greater than 3/64 inch wide by 1/2 inch long.

SINGLE-ADDRESS MESSAGE— A message with only one addressee.

SPECIAL-HANDLING MARKINGS— Additional markings or designations on some messages that alert the user or communications center that the message requires special attention in handling. Some of these include Caveat, Restricted Data (RD), Formerly Restricted Data (FRD), FOUO, EFTO, SPECAT, and PERSONAL FOR.

SWS (SENIOR WATCH SUPERVISOR)— When assigned, the senior enlisted person on watch responsible for handling all communications matters; responsible to the CWO.

T

TECH CONTROL SUPERVISOR— Responsible for establishing and maintaining required circuits, including initiating actions to restore or bypass failed equipment, quality monitoring, supervising assigned personnel, and controlling procedures for all systems; responsible to the CWO.

TELEPROCESSING— A method of data processing in which communications devices are used.

TERMINATION REQUEST MESSAGE— A message sent to request establishment of circuits with a NCTAMS or NAVCOMTELSTA on a limited or fill-time basis.

TIME SHARING— A processing mode in which users share computer system resources through online terminals.

TSCO (TOP SECRET CONTROL OFFICER)— An officer, senior noncommissioned officer (E-7, E-8, or E-9) or a civilian employee, (GS-7 or above) who is responsible for the receipt, custody, accounting, and disposition of Top Secret material within the command.

TSO (TELECOMMUNICATIONS SERVICE ORDER)— Used to authorize the start, change, or discontinue circuits, trunks, links, or systems.

TSR (TELECOMMUNICATIONS SERVICE REQUEST)—Initiates additions, deletions, or changes from the originating command to existing Defense Communications System (DCS) circuits.

TVA (TEMPEST VULNERABILITY ASSESSMENT)— The vulnerability of a ship, aircraft, shore station transportable equipment, or a contractor facility to susceptibility, environment, and threat.

TVAR (TEMPEST VULNERABILITY ASSESSMENT REQUEST)— A request submitted prior to processing classified data to the Naval Criminal Investigation Service.

Y

YANKEE PRECEDENCE— This category is in addition to the four major precedences categories; it is an EMERGENCY COMMAND PRECEDENCE (ECP). It is identified by the precedence prosign "Y" and limited to designated emergency action command and control messages. Speed of service objective is not fixed. Handled as fast as humanly possible with an objective of less than 10 minutes.

APPENDIX II

GLOSSARY OF ACRONYMS AND ABBREVIATIONS

A

ACP— Allied communications publication.
AIG— Address indicating group.
AIS— Automated information system.
ALCOM— All commands.
ALNAV— All Navy.
AMCROSS— American Red Cross.
ATP– Allied tactical publication.
AUTODIN— Automatic Digital Network.
AXP— Allied exercise publication.

B

BKS— Broadcast keying station.
BSR— Broadcast screening request.

C

CE— Compromising emanations.
CIB— Communications Information Bulletin.
CIC— (1) Content Indicator Code (2) Combat Information Center.
CINCLANTFLT— Commander in Chief, Atlantic Fleet.
CINCPACFLT— Commander in Chief, Pacific Fleet.
CMS— Communications Security Material System.
CNO— Chief of Naval Operations.
COMMAREA— Communications area.
COMMO— Communications Officer.
COMMSHIFT— Communications shift.
COMMSPOT— Communications spot report.
COMNAVCOMTELCOM— Commander, Naval Computer and Telecommunications Command.
COMNAVSECGRU— Commander, Naval Security Group.
COMNAVSURFLANT— Commander, Naval Surface Forces Atlantic.
COMSEC— Communications security.
COSIR— Cite our service in return.
CP— Change proposal.
CRT— Cathode-ray tube.
CWO— Communications Watch Officer.

D

DCS– (1) Defense Courier Service (2) Defense Communications Service.
DCMS— Director, Communications Security Material System.
DESRON— Destroyer squadron.
DISA— Director, Information Security Agency.
DON— Department of the Navy.
DODCAF— Department of Defense Central Adjudication Facility.
DSCS— Director, Satellite Communications System.
DSR— Data speed reader.
DTG— Date-time group.

E

EA— Electronic attack (replaces electronic countermeasures (ECM)).
EAM— Emergency Action Message.
EASTPAC— Eastern Pacific.
ECP— Emergency command precedence.
EFTO— Encrypt for transmission only.
EMCON— Emanation control.
EOJ— End of job.
EP— Electronic protection (replaces electronic counter-countermeasures (ECCM)).

F

FC— Fixed-cycle.
FCC— Federal Communications Commission.
FIFO— First-in, first-out.
FLTCINC— Fleet Commander in Chief.
FOTP— Fleet Operational Telecommunications Program.
FOUO— For Official Use Only.
FRD— Formerly Restricted Data.
FTOC— Fleet Telecommunications Operations Center.
FTP— Fleet training publication.
FXP— Fleet exercise publication.

G

GENADMIN— General Administrative.
GHz— Gigahertz.
GMT— Greenwich Mean Time.

H

HF— High frequency.
HW— Hardware.

I

IDL— International Date Line.
IDS— Intrusion Detection System.
IFF— Identification, friend or foe.
INMARSAT— International Maritime Satellite System.
IR— Information resources.
ISSM— Information Systems Security Manager.
ISSO— Information Systems Security Officer.
ITS— Instrumented TEMPEST Survey.

J

JANAP— Joint Army-Navy-Air Force Publication.
JCS— Joint Chiefs of Staff.

K

kHz— Kilohertz.

L

LANT— Atlantic.
LDMX— Local Digital Message Exchange.
LIMDIS— Limited distribution.
LMF— Language and media format.
LOEP— List of effective pages.

M

MARS— Military Affiliate Radio System.
MED— Mediterranean.
MIJI— Meaconing, Interference, Jamming, and Intrusion.
MTF— Message text format.

N

NARDAC— Naval Regional Data Automation Center.
NATO— North Atlantic Treaty Organization.
MMAREA— Naval communications area.
NAVCOMPARS— Naval Communications Processing and Routing System.
NAVCOMTELDET— Naval Computer and Telecommunications Detachment.
NAVCOMTELCOM— Naval Computer and Telecommunications Command.
NAVCONTELSTA— Naval Computer and Telecommunications Station.
NAVDAC— Naval Data Automation Center.
NAVDAF— Naval Data Automation Facility.
NAVELEXSECCEN— Naval Electronics Security Center.
NAVEMSCEN— Naval Electromagnetic Spectrum Center.
NAVOP— Naval Operations.
NAVSECGRUDEPT— Naval Security Group Department.
NAVTELCOM— Naval Telecommunications Command.
NCS— (1) Naval Communications Station (2) National Communications System (3) Net Control Station.
NCTAMS— Naval Computer and Telecommunications Area Master Station.
NCTS— Naval Computer and Telecommunications Station.
NIF— Naval Industrial Fund.
NMC— Numerical message correction.
NOTAM— Notice to airmen.
NSO— Network Security Officer.
NTIA— National Telecommunications and Information Administration.
NTP— Naval telecommunications publication.
NTS— Naval Telecommunications System.
NWPC— Naval warfare publications custodian.
NWPL— Naval Warfare Publications Library.
NWP— Naval warfare publication.

O

OPORD— Operation Order.
OSRI— Originating station routing indicator.
OTAR— Over-the-air rekey.
OTAT— Over-the-air transfer.

P

PCMT— Personal Computer Message Terminal.
PC— Personal computer.
PLA— Plain Language Address.

PQS— Personnel Qualification Standards.
PRO FORMA— Predetermined format.
PROSIGNS— Procedural signs.
PSN— Processing sequencing number.

R

RADAY— Radio day.
RD— Restricted Data.
RI— Routing indicator.
RMKS— Remarks.

S

SEF— SPECAT Exclusive For.
SIGSEC— Signal security.
SIOP-ESI— Single Integrated Operational Plan-Extremely Sensitive Information.
SOG— Special Operating Group.
SOP—Standard operating procedure.
SPECAT— Special Category.
SSN— Station serial number.
SUBMISS— Submarine missing.
SUBRON— Submarine squadron.
SUBSUNK— Submarine sunk.
SVC— Service.
SWS— Senior Watch Supervisor.

T

TASO— Terminal Area Security Officer.
TCC— Telecommunications Center.
TICON— Tight control.
TOD— Time of delivery.
TOF— Time of file.
TOR— Time of receipt.
TPI— Two-person integrity.
TR— Trouble report.
TSC— Top Secret control officer.
TSEC— Telecommunications security.
TSO— Telecommunications service order.
TSR— Telecommunications service request.
TVA— TEMPEST Vulnerability Assessment.
TVAR— TEMPEST Vulnerability Assessment Request.

U

UPS— Uninterrupted power supply.
US&P— United States and Possessions.
USMCEB— United States Military Communications-Electronics Board.

V

VDT— Video display terminal.

W

WESTPAC— Western Pacific.

Z

ZDK— Send again (“Z” signal).
ZUI— Your attention is invited to . . . (“Z” signal).

APPENDIX III

REFERENCES USED TO DEVELOP THE TRAMAN

Allied Call Sign and Address Group System–Instructions and Assignments, ACP 100(F), Joint Chiefs of Staff, Washington, DC, March 1984.

Automatic Digital Network (AUTODIN) Operating Procedures, JANAP 128(J), Joint Chiefs of Staff, Washington, DC, July 1993.

Bask Operational Communications Doctrine (U), NWP 4 (Rev. B) (NWP 6-01), Chief of Naval Operations, Washington, DC, September 1989.

Communication Instructions General (U), ACP 121(F), Joint Chiefs of Staff, Washington, DC, April 1983.

Communications Instructions—General, ACP 121 US SUPP-1(F), Joint Chiefs of Staff, Washington, DC, June 1981.

Communications Instructions Security (U), ACP 122, Joint Chiefs of Staff, Washington, DC, 1981.

Communication Instructions—Operating Signals, ACP 131(D), Joint Chiefs of Staff, Washington, DC, May 1986.

Communications Instuctions–Tape Relay Procedures, ACP 127(G), Joint Chiefs of Staff, Washington, DC, November 1988.

Communications Instructions–Teletypewriter (Teleprinter) Procedures, ACP 126(C), Joint Chiefs of Staff, Washington, DC, May 1989.

Communications Security Material System (CMS) Policy and Procedures Manual, CMS 1, Department of the Navy, Washington, DC, March 1993.

Department of the Navy Automated Information Systems (AIS) Security Program, SECNAVINST 5239.2, Secretary of the Navy, Washington, DC, November 1989.

Department of the Navy Information and Personnel Security Program Regulation, OPNAVINST 5510.1H, Chief of Naval Operations, Washington, DC, May 1991.

Department of the Navy Physical Security and Loss Prevention, OPNAVINST 5530.14B, Chief of Naval Operations, Washington, DC, December 1988.

Department of the Navy Privacy Act (PA) Program, SECNAVINST 5211.5D, Secretary of the Navy, Washington, DC, July 1992.

Department of the Navy Security Program for Automatic Data Processing Systems, OPNAVINST 5239.1A, Chief of Naval Operations, Washington, DC, August 1982.

Fleet Communications (U), NTP 4(C), Commander, Naval Telecommunications Command, Washington, DC, June 1988.

Fleet Telecommunications Procedures for Atlantic and Mediterranean Naval Communications Areas, NCTAMS LANT/MEDINST C2300.1, Naval Computer and Telecommunications Area Master Station LANT/Naval Computer and Telecommunications Area Master Station MED, September 1993.

Fleet Telecommunications Procedures for the Pacific and Indian Ocean Naval Communication Areas, NCTAMSEASTPAC/NCTAMS WESTPACINST C2000.3D, Naval Computer and Telecommunications Area Master Station EASTPAC/Naval Computer and Telecommunications Area WESTPAC, 10 August 1992.

Guideline for Automatic Data Processing Risk Analysis, Federal Information Processing Standards (FIPS) Publication 65, Department of Commerce, National Bureau of Standards, Springfield, VA, August 1979.

Guideline for Evaluation of Techniques for Automated Personal Identification, Federal Information Processing Standards (FIPS) Publication 48, Department of Commerce, National Bureau of Standards, Springfield, VA, April 1977.

Hussain, Donna, and K. M. Hussain, *Managing Computer Resources*, Second Edition, Richard D. Irwin, Inc., Homewood, IL, 1988.

Local SOP and PQS, Bureau of Naval Personnel (PERS-1043B), Washington, DC.

Local SOP and PQS, Enlisted Program Management Center (EPMAC), New Orleans, LA.

Local SOP and PQS, USS EISENHOWER (CVN-69).

Local SOP and PQS, USS NASSAU (LHA-4).

Message Address Directory, Joint Chiefs of Staff, Washington, DC, June 1990.

Naval Warfare Documentation Guide, NWP 0 (Rev. P) (NWP 1-01), Chief of Naval Operations, Washington, DC, January 1990.

Operational Reports, NWP 10-1-10 (NWP 1-03.1), Chief of Naval Operations, Washington, DC, November 1987.

Security Requirements for Automated Information Systems (AISs), DODD 5200.28, Deputy Security of Defense, Washington, DC, March 1988.

Telecommunications Users Manual, NTP 3(1), Commander, Naval Telecommunications Command, Washington, DC, January 1990.

U.S. Call Sign & Address Group System Instructions & Assignments, ACP 100 U.S. SUPP-1(N), Joint Chiefs of Staff, Washington, DC, June 1989.

U.S. Navy Address Indicating Group (AIG) and Collective Address Designator (CAD) Handbook, NTP 3 SUPP-1(K), Commander, Naval Telecommunications Command, Washington, DC, August 1986.

INDEX

A

AIG, 2-18
AIS disaster protection, 4-18
  fire safety, 4-18
  supporting utilities protection, 4-21
AIS facility physical protection, 4-23
AIS media protection measures, 4-11
  disposition of media, 4-12
  security controls, 4-11
  security markings, 4-12
AIS security, 4-1
  authoritative references, 4-13
  contingency planning, 4-26
  data privacy, 4-33
  disaster protection, 4-18
  plan documentation, 4-13
  program implementation, 4-13
  program planning, 4-13
  security inspections, 4-30
  threats and risk analysis, 4-14
AIS security concepts, 4-1
  AIS assets, 4-2
  countermeasures, 4-4
  likelihood and risk, 4-3
  threats, 4-2
  vulnerability, 4-2
  successful attacks/adverse events, 4-2
AIS security goal, 4-1
AIS security program, 4-6
AIS security staff, 4-6
  information systems security manager (ISSM), 4-6
  information systems security officer (ISSO), 4-7
  command security manager, 4-7
  network security officer (NSO), 4-7
  terminal area security officer (TASO), 4-7
AIS service request, 1-5
AIS threats and risk analysis, 4-14
Annual loss expectancy, 4-16
Attacks, 4-2
Automated scheduling systems, 1-40

B

Backup plans, 4-5,4-28
Backup operations, 4-28
Batch, 1-9, 1-12
Boundary protection, 4-23
BSR, 2-24

C

CAD, 2-18
CIBs, 2-36
Classified data, 4-10
  controlled security mode, 4-11
  dedicated security mode, 4-10
  multilevel security mode, 4-10
  system high security mode, 4-10
Classified material, 5-6
  clearing media and hardware, 5-10
  handling, 5-6
Classified material destruction, 5-10
  routine, 5-10
  procedures, 5-10
  reports, 5-10
  types, 5-10
Classified material destruction types, 5-10
  burning, 5-11
  shredding, 5-11
  pulverizing, 5-11
  disintegrating, 5-11
  jettisoning/sinking, 5-11
Classified material handling, 5-6
  SPECAT/Top Secret and above, 5-8
  AIS, (classified) 5-10
  Confidential, 5-10
  Secret, 5-10

Classified material handling—Continued
Top Secret, 5-8
Top Secret control officer (TSCO), 5-6
Classified material handling of SPECAT/Top Secret and above, 5-8
destruction, 5-8
verification, 5-8
CMS, 2-10
CMS alternate, 3-2
CMS custodian, 2-10, 3-2
CMS local holder, 3-2
CMS user, 3-2
CMS witness, 3-2
Command communications organization, 2-9
CMS custodian, 2-10
commanding officer, 2-9
communications center supervisor, 2-10
communications officer, 2-9
CWO, 2-10
radio officer, 2-9
technical control supervisor, 2-10
Command ship communications, 2-11
Commander, Naval Computer and Telecommunications Command (COMNAVCOMTELCOM), 2-3
COMMSHIFT, 2-24
COMMSPOT, 2-24
Communications (COMM), 4-6
Communications center files, 2-25
broadcast file, 2-25
commercial traffic file, 2-25
cryptocenter file, 2-25
embarked command file, 2-25
facsimile file, 2-25
file fillers, 2-26
file maintenance, 2-26
general message file, 2-25
master file, 2-25
NATO/allied files, 2-26
retention of files, 2-26
SPECAT SIOP-ESI file, 2-25
station file, 2-25
Communications center supervisor, 2-10
Communications management, 2-6
evaluating performance, 2-6
general administration, 2-7
office management, 2-7
personnel management, 2-7
responsibilities, 2-7
Communications Officer, 2-10
Communications material accounting general reports, 3-3
destruction, 3-3, 3-8
receipt, 3-3
transfer, 3-3
Communications material accounting general reports destruction, 3-3, 3-8
CMS 25 one-time keying material destruction report, 3-4
CMS 25B COMSEC keying material local destruction report, 3-6
CMS 25MC COMSEC keying material local report, 3-8
regular, 3-3
Communications material accounting inventory reports, 3-3
combined SF-153, 3-3
fixed-cycle, 3-3
special SF-153, 3-3
Communications material accounting reports, 3-3
general, 3-3
inventories, 3-3
Communications planning, 2-27
communications plan, 2-28
EP and EA, 2-28
frequency management, 2-29
protection, 2-28
requirements, 2-27
spectrum management, 2-29
telecommunications service order (TSO), 2-29
telecommunications service request (TSR), 2-29
Communications planning frequency management, 2-29
allocation, 2-29
assignment, 2-29

Communications security, 3-1
authentication, 3-11
Communications Security Material System (CMS), 2-10, 3-1
equipment, 3-11
MIJI, 3-12
personnel, 3-2
responsibilities, 3-2
transmission security, 3-11
Communications security authentication, 3-11
challenge and reply, 3-11
transmission, 3-11
Communications security MIJI, 3-12
harmful interference, 3-12
interference, 3-12
intrusion, 3-12
jamming, 3-12
meaconing, 3-12
Communications security personnel, 3-2
CMS alternate, 3-2
CMS custodian, 3-2
CMS local holder, 3-2
CMS user, 3-2
CMS witness, 3-2
Communications security responsibilities, 3-2
inventory, 3-3
receipt, 3-3
storage, 3-2
training, 3-2
Communications security transmission security, 3-11
destruction, 3-8
equipment, 3-11
OTAT/OTAR, 3-11
two-person integrity (TPI), 3-9
Communications Security Material System (CMS)
complete destruction, 3-9
effective keying material, 3-9
keying material, 3-9
superseded keying material, 3-9
Communications Security Material System (CMS) destruction, 3-8
complete, 3-9
Communications Security Material System (CMS) destruction—Continued
emergency, 3-8
precautionary, 3-8, 5-12
routine, 3-8
verify, 3-9
Communications Security Material System (CMS) precautionary destruction, 3-8
keying, 3-9
nonessential, 3-9
Communications watch officer (CWO), 2-10
Compromising emanations, 3-1, 5-1
Computer operations, 1-4, 1-10
Contingency plan, 1-14, 1-26, 4-5, 4-26
Contingency planning, 4-26
COOP backup planning, 4-28
COOP testing, 4-30
emergency response planning, 4-26
recovery planning, 4-29
COOP, 4-26
backup planning, 4-28
testing, 4-30
Countermeasures, 4-4
administrative controls, 4-4
managerial controls, 4-4
physical controls, 4-4
technical controls, 4-4
Cryptographic operations, 3-10
crypto, 3-10
cryptoinformation, 3-10
cryptomaterial, 3-10
crypto-related information, 3-10
cryptosystem, 3-11
cryptovariables, 3-11
responsibilities, 3-11
terms, 3-10
Cryptosecurity, 3-1
operations and requirements, 3-1
Customer/user reports, 1-21
CWO, 2-10

D

Data, 4-6

Data entry, 1-2, 1-6, 1-12
Data privacy, 4-33
identification techniques, 4-39
information management practices, 4-37
personal data risk assessment, 4-36
personal data security risks, 4-36
Data protection measures, 4-10
classified data, 4-10
sensitive unclassified data, 4-11
unclassified data, 4-11
DCS, 2-2
Defense Communications System, 2-2
Defense Information System Agency, 2-2
Destruction of classified material, 5-10
DISA, 2-2
Downtime, 1-19, 1-20, 1-23

E
EAM, 2-31
EFTO, 2-30
Emanations protection, 4-24
EMCON, 5-2
Emergency plans, 5-11
fire, 5-12
precautionary, 3-8, 5-12
priorities, 5-12
Emergency response planning, 4-26

F
Fire safety, 4-18
facility fire exposure, 4-19
fire detection, 4-20
fire extinguishment, 4-21
Flagship (See command ship communications), 2-11
FOUO, 2-30
FRD, 2-30

G
GMT, 2-19

H
Help-desk support, 1-20
Human resources, 4-6

I
Information needs, 1-14
Initial scheduling phase, 1-10
Interior physical protection, 4-24
I/O control, 1-2, 1-10, 1-12, 1-16
I/O control clerk, 1-2, 1-6, 1-18, 1-21

J
Job control log, 1-4
Job dependencies, 1-16
Job monitoring, 1-6
Job preparation, 1-6
control parameters, 1-6
output requirements, 1-6
run sheet, 1-6

L
LIMDIS, 2-30
Loss potential estimates, 4-14

M
Management reports, 1-21
Managing production, 1-8
MARS, 2-5
Media library, 1-2, 1-12
Message and routing address types, 2-17
broadcast screening request (BSR), 2-24
communications guard shift (COMMSHIFT), 2-24
communications spot (COMMSPOT), 2-24
service, 2-23
termination requests, 2-24
tracer, 2-24
Message and routing addresses, 2-17
address group, 2-17
address indicating groups (AIGS), 2-18
collective address designator (CAD), 2-18
message addresses, 2-17
routing indicators, 2-17
special operating groups (SOGs), 2-12
types, 2-23

Message elements, 2-19
conversion of GMT/local time, 2-20
DTG, 2-19
Greenwich mean time (GMT), 2-19
Julian date, 2-20
time, 2-19
Message logs, 2-12
central message log, 2-12
circuit logs, 2-12
journal logs, 2-15
Top Secret control log, 2-12
Message precedences, 2-20
FLASH, 2-20
IMMEDIATE, 2-20
PRIORITY, 2-20
ROUTINE, 2-20
YANKEE, 2-20
Message readdressals, 2-22
Message user responsibilities, 2-22
drafter, 2-22
originator, 2-22
releaser, 2-22
MIJI, 3-12
Military Affiliate Radio System (MARS), 2-5
Minimize, 2-23, 2-31
Multiprocessing, 1-9
Multiprogramming, 1-9, 1-10

N

National Communications System (NCS), 2-1
Naval communications, 2-1
command organization, 2-1
commander, 2-2
mission, 2-2
NAVCOMTEL DET, 2-5
NAVCOMTELSTA, 2-4
NAVDAF, 2-5
NCTAMS, 2-4
policy, 2-2
telecommunication system, 2-2
Naval Communications Area, 2-4
Naval Computer and Telecommunications Area Master Station (NCTAMS), 2-4
Naval Computer and Telecommunications Detachment (NAVCOMTEL DET), 2-5
Naval Computer and Telecommunications Station (NAVCOMTELSTA), 2-5
Naval Data Automation Command (NAVDAC), 2-3
Naval Data Automation Facility (NAVDAF), 2-5
Naval messages, 2-19
classes, 2-23
message readdressals, 2-22
types, 2-23
Naval Security Group Departments (NAVSECGRUDEPTS), 2-5
Naval Telecommunications System, 2-2
Naval Warfare Publications Library (NWPL), 2-32
administration, 2-32
binders, 2-34
clerk, 2-32
custodian, 2-32
entry of changes, 2-35
extracts, 2-35
maintenance, 2-32
publication notice, 2-35
publications, 2-35
watch-to-watch inventory, 2-35
Naval Warfare Publications Library (NWPL) publications, 2-36
allied communications, 2-36
communications information bulletins (CIBs), 2-36
fleet telecommunications, 2-36
Joint Army-Navy-Air Force, 2-36
naval telecommunications, 2-36
naval warfare, 2-36
receiving or revised, 2-36
NAVCOMMAREA, 2-4
NCS, 2-1
Networking, 1-9
NTS, 2-2
NWPL, 2-32

O
Online processing, 1-9
Operating system, 1-9, 1-10, 1-22
Operation orders, 2-3
OPORDs, 2-3, 2-11
OTAR, 3-11
OTAT, 3-11
Output products, 1-1, 1-4

P
Physical security, 4-8, 5-4
  cipher locks, 5-5
  combinations, 5-4
  containers, 5-4
  data file protection, 4-8
  natural disaster protection, 4-8
  physical access controls, 4-8
  physical security protection, 4-8
  storage, 5-4
Physical security measures, 4-8
  environmental security, 4-8
  fire protection, 4-9
  hardware protection, 4-10
  lighting, 4-8
  physical security, 4-8
  physical structure security, 4-9
  power supply protection, 4-9
Postcomputer processing, 1-9
Precomputer processing, 1-9
Priorities, 1-9, 1-16
Processing time, 1-14
Production control, 1-10, 1-21
  daily operations, 1-21
  output reports, 1-21
  production control coordinator, 1-8, 1-9, 1-17
Production control and scheduling, 1-27
Production processing, 1-19
  application program processing errors, 1-19
  help-desk support, 1-20
  system downtime, 1-20
Production scheduling, 1-17
  monthly, 1-17
  workload schedule development, 1-18

Q
Quality control, 1-12

R
Radio officer, 2-9
RD, 2-30
Recovery, 4-29
  emergency response planning, 4-26
  planning, 4-29
Remedial measures selection, 4-16
Remote terminal areas protection, 4-24
Risk analysis, 4-14
Risk management, 4-4

S
Scheduler, 1-2, 1-8, 1-13
Scheduling, 1-2, 1-19
Scheduling methods, 1-14, 1-16
Scheduling process, 1-13
Scope of AIS security, 4-6
  management responsibility, 4-6
  personal responsibility, 4-7
Security, See AIS security.
Security, 5-3
  areas, 5-3
  classification, 5-6
  handling, 5-6
  physical, 5-4
Security areas, 5-3
  access, 5-3
  access list, 5-3
  restricted, 5-3
  sanitizing, 5-3
  visitor's log, 5-4
Security handling, 5-6
  after working hours, 5-7
  personnel, 5-7
  working hours, 5-7
Security inspections, 4-30
  conducting inspections, 4-32
  inspection follow-up, 4-33
  inspection plan, 4-31
  inspection preparation, 4-31

Security markings, 4-12
CRT displays, 4-12
hard-copy reports, microfilm, and microfiche, 4-12
magnetic media, 4-12
Security modes, 4-10
controlled, 4-11
dedicated, 4-10
multilevel, 4-10
system high, 4-10
Security survey, 4-24
Senior Watch Supervisor (SWS), 2-10
Service Message, 2-23
SOGs, 2-18
SPECAT, 2-25, 2-30, 5-6
Special handling markings, 2-30, 5-5
allied restricted, 2-31, 5-6
caveat, 2-30
Encrypted for Transmission Only (EFTO), 2-30, 5-6
For Official Use Only (FOUO), 2-30, 5-6
Formerly Restricted Data (FRD), 2-30, 5-5
JCS Emergency Action Message (EAM), 2-31
Limited Distribution (LIMDIS), 2-30, 5-5
MINIMIZE considered, 2-31
NATO Restricted, 2-31, 5-6
PERSONAL FOR, 2-31, 5-6
Restricted Data (RD), 2-30, 5-5
Special Category (SPECAT), 2-25, 2-30, 5-6
Special-handling markings for Special Category (SPECAT), 2-25, 2-30, 5-6
SIOP-ESI, 2-31
PSEUDO, 2-31
Standard Operating Procedures (SOPS) 2-12
Supporting utilities protection, 4-21

T

Technical control supervisor, 2-10
Teleprocessing, 1-9
TEMPEST, 5-2
compromising emanations (CE), 5-2
TEMPEST vulnerability assessment (TVA), 5-2
TEMPEST vulnerability assessment report (TVAR), 5-2
TEMPEST vulnerability assessment (TVA), 5-2
environment, 5-2
susceptibility, 5-2
threat, 5-2
Threat analysis, 4-15
Time sharing, 1-9
TPI, 3-9
Tracer message, 2-24
TSCO, 5-6
TSO, 2-29
TSR, 2-29
TVA, 5-2
TVAR, 5-2

U

Uninterrupted power source (UPS), 4-9
Uninterrupted power supply (UPS), 4-22
User support, 1-7
logistical support, 1-8
trouble calls, 1-8
user inquiries, 1-7

*U.S. Government Printing Office: 1998 - 633-154/60099

RADIOMAN TRAINING SERIES
MODULE 1 - ADMINISTRATION AND SECURITY

NAVEDTRA 12845

Prepared by the Naval Education and Training Professional Development and Technology Center (NETPDTC), Pensacola, Florida

Congratulations! By enrolling in this course, you have demonstrated a desire to improve yourself and the Navy. Remember, however, this self-study course is only one part of the total Navy training program. Practical experience, schools, selected reading, and your desire to succeed are also necessary to successfully round out a fully meaningful training program. You have taken an important step in self-improvement. Keep up the good work.

HOW TO COMPLETE THIS COURSE SUCCESSFULLY

ERRATA: If an errata comes with this course, make all indicated changes or corrections before you start any assignment. Do not change or correct the associated text or assignments in any other way.

TEXTBOOK ASSIGNMENTS : The text pages that you are to study are listed at the beginning of each assignment. Study these pages carefully before attempting to answer the questions in the course. Pay close attention to tables and illustrations because they contain information that will help you understand the text. Read the learning objectives provided at the beginning of each chapter or topic in the text and/or preceding each set of questions. In the course. Learning objectives state what you should be able to do after studying the material. Answering the questions correctly helps you accomplish the objectives.

SELECTING YOUR ANSWERS: After studying the associated text, you should be ready to answer the questions in the assignment. Read each question carefully, then select the BEST answer. Be sure to select your answer from the subject matter in the text. You may refer freely to the text and seek advice and information from others on problems that may arise in the course. However, the answers must be the result of your own work and decisions. You are prohibited from referring to or copying the answers of others and from giving answers to anyone else taking the same course. Failure to follow these rules can result in suspension from the course and disciplinary action.

ANSWER SHEETS: You must use answer sheets designed for this course (NETPMSA Form 1430/5, Stock Ordering Number 0502-LP-216-0100). Use the answer sheets provided by Educational Services Officer (ESO), or you may reproduce the one in the back of this course booklet.

SUBMITTING COMPLETED ANSWER SHEETS: As a minimum, you should complete at least one assignment per month. Failure to meet this requirement could result in disenrollment from the course. As you complete each assignment, submit the completed answer sheet to your ESO for grading. You may submit more than one answer sheet at a time.

GRADING : Your ESO will grade each answer sheet and notify you of any incorrect answers. The passing score for each assignment is 3.2. If you receive less than 3.2 on any assignment, your ESO will list the questions you answered incorrectly and give you an answer sheet marked

"RESUBMIT." You must redo the assignment and complete the RESUBMIT answer sheet. The maximum score you can receive for a resubmitted assignment is 3.2.

COURSE COMPLETION: After you have submitted all the answer sheets and have earned at least 3.2 on each assignment, your command should give you credit for this course by making the appropriate entry in your service record.

NAVAL RESERVE RETIREMENT CREDIT: If you are a member of the Naval Reserve, you will receive retirement points if you are authorized to receive thereunder current directives governing retirement of Naval Reserve personnel. For Naval Reserve retirement, this course is evaluated at 8 points. (Refer to BUPERSINST 1001.39 for more information about retirement points.)

STUDENT QUESTIONS: If you have questions concerning the administration of this course, consult your ESO. If you have questions on course content, you may contact NETPDTC at:

DSN: 922-1501
Commercial: (904) 452-1501
FAX: 922-1819
INTERNET:
n311.products@smtp.cnet.navy.mil

COURSE OBJECTIVES: In completing this nonresident training course, you will demonstrate a knowledge of the subject matter by correctly answering questions on the following subjects:

AIS Administration, Communications Administration, Communications Security, AIS Security, and General Security.

Naval courses may include several types of questions--multiple-choice, true-false, matching, etc. The questions are not grouped by type but by subject matter. They are presented in the same general sequence as the textbook material upon which they are based. This presentation is designed to preserve continuity of thought, permitting step-by-step development of ideas. Not all courses use all of the types of questions available. You can readily identify the type of each question, and the action required, by reviewing of the samples given below.

MULTIPLE-CHOICE QUESTIONS

Each question contains several alternative answers, one of which is the best answer to the question. Select the best alternative, and blacken the appropriate box on the answer sheet.

SAMPLE

s-1. The first U.S. Navy nuclear-powered vessel was what type of ship?

1. Carrier
2. Submarine
3. Destroyer
4. Cruiser

Indicate in this way on your answer sheet:

	1	2	3	4
	T	F		
s-1	☐	■	☐	☐

TRUE-FALSE QUESTIONS

Mark each statement true or false as indicated below. If any part of the statement is false, the entire statement is false. Make your decision, and blacken the appropriate box on the answer sheet.

SAMPLE

s-2. Shock will never be serious enough to cause death.

1. True
2. False

Indicate in this way on your answer sheet:

	1	2	3	4
	T	F		
s-2	☐	■	☐	☐

MATCHING QUESTIONS

Each set of questions consists of two columns, each listing words, phrases or sentences. Your task is to select the item in column B which is the best match for the item in column A. Items in column B may be used once, more than once, or not at all. Specific instructions are given with each set of questions. Select the numbers identifying the answers and blacken the appropriate boxes on your answer sheet.

SAMPLE

In answering questions s-3 through s-6, SELECT from column B the department where the shipboard officer in column A functions. Responses may be used once, more than once, or not at all.

A. OFFICER	B. DEPARTMENT
s-3. Damage Control Assistant	1. Operations Department
s-4. CIC Officer	2. Engineering Department
s-5. Disbursing Officer	3. Supply Department
s-6. Communications Officer	4. Navigation Department

Indicate in this way on your answer sheet:

	1	2	3	4
	T	F		
s-3	☐	■	☐	☐
s-4	■	☐	☐	☐
s-5	☐	☐	■	☐
s-6	■	☐	☐	☐

ASSIGNMENT 1

Textbook Assignment: "AIS Administration," chapter 1, pages 1-1 through 1-28.

1-1. You are working as an I/O control clerk. Before accepting a job for processing on the computer, you should look over the transmittal form to ensure which of the following criteria is met?

1. All copies have been filed
2. All entries are readable and understandable
3. All required outputs have been specified
4. All SCL statements are in the proper sequence

1-2. Computer operations has just informed you that the payroll update (a series of 18 jobs) is finished and ready for pickup. Upon receiving the output, you should take what action immediately?

1. Use the burster
2. Log the jobs out
3. File the jobs
4. Check the output products

1-3. As an I/O control clerk, you will NOT be expected to perform which of the following tasks?

1. Make SCL changes to production run streams
2. Monitor jobs to ensure all data-are processed
3. Reconcile processing discrepancies and inconsistencies
4. Assist the computer operator in setting up production jobs

1-4. As an I/O control clerk, you can be expected to operate a variety of equipment, such as copying machines, and terminals. These are known as what type of equipment?

1. Online
2. Auxiliary
3. Secondary
4. Independent

1-5. On the transmittal form, the block marked "OPERATIONS USE ONLY" contains which of the following items of information?

1. Job/task number
2. Computer to be used
3. Type of operation performed
4. When the job was accepted

1-6. As an I/O control clerk, one of your jobs will be to keep an up-to-date record of all jobs received for processing. What document should you use?

1. A run schedule
2. A job schedule
3. A pass down log
4. A job control log

1-7. If the input that comes with a job becomes misplaced or lost, you still have means of tracking it down by lookinq in what control log entry?

1. Program name
2. Type of input
3. Input forwarded
4. Computer system

1-8. To properly prepare the user's input for processing, you as I/O control clerk must have a certain amount of information available, such as computer run sheet, how to make up control or SCL statements, and any special output requirements the job may call for. This information can be found in the

1. run book
2. job manual
3. task folder
4. master run manual

1-9. A run sheet to be used by the computer operator should contain which of the following information?

1. Breakpoints
2. Partition numbers
3. Recovery procedures
4. List of required inputs

1-10. If a job terminates before going to a normal EOJ, you as the I/O control clerk may be required to collect which of the following data/information?

1. Output data and memory dump only
2. Input data and SCL statements only
3. Input data, output data, and memory dump
4. Output data, console printout, and SCL statements

1-11. During the SUADPS daily update for supply, problems reading the current master read file (MRF) on disk drive 241 are encountered. The job terminates prematurely, leaving eight jobs to be run. The computer operator calls on you as the I/O control clerk to help in the recovery process. You can be expected to perform all except which of the following tasks?

1. Provide the operator with the input parameters and/or SCL statements to recover the job
2. Remove the defective disk pack from drive 241 and forward it to the technicians to be checked out
3. See to it that the remaining jobs are rescheduled once the master file is recreated, and notify the user
4. Provide the operator with the file identification number needed to recover the MRF file

1-12. As an I/O control clerk, to determine that a job ran successfully and that all processing steps were properly carried out, you should review what document?

1. The pass down log
2. The computer run sheet
3. The confirmation report
4. The computer console printout

1-13. As an I/O control clerk, what document provides you with a list of all the error conditions and messages for all jobs run on the computer during a work shift?

1. The error/discrepancy report
2. The computer console printout
3. The error message log
3. The rerun report

1-14. As an I/O control clerk, you may be responsible for reconciling processing discrepancies . To determine the problem, which of the following documents will usually provide you with the information you need?

1. The pass down log
2. The computer run sheet
3. The confirmation report
4. The computer console printout

1-15. As an I/O control clerk, you are checking over the user's output products and need to verify that all items requested were produced. To do this, you should refer to which of the following sources?

1. The run manual
2. The task folder
3. The user manual
4. The instruction folder

1-16. As an I/O control clerk, once you have packaged the user's output products and placed them in the pick-up area, you should log the job out in which of the following logs?

1. The job control log
2. The user's job log
3. The production log
4. The EOJ/pick-up log

1-17. As an I/O control clerk, if during the process of checking over the user's output products, you happen to come across an error, you should carry out which of the following actions?

1. Log the job out, and inform the user of the error at the time of pickup only
2. Bring the error to the attention of your superior, then log the job out with the appropriate comments only
3. Reschedule the job as if nothing has happened, and notify the user there will be a slight delay
4. Pull the job immediately, bring the error to the attention of your superior so the job may be rescheduled, and notify the user

1-18. As an I/O control clerk, You will be involved with and communicating with the user. Which of the following communications skills must you possess in order to maintain a good relationship with the user?

1. Refer problems to users
2. Explain problems only
3. Understand requests only
4. Understand requests and explain problems

1-19. A scheduler does NOT perform which of the following tasks?

1. Review AIS requests
2. Prepare schedules
3. Operate the computer to run production jobs
4. Organize data processing priorities for both scheduled and unscheduled work

1-20. What method should you use to determine the accuracy of your schedules?

1. Monitor the jobs
2. Review production results
3. Supervise computer operations
4. Review job control logs

1-21. To determine how to go about scheduling work on your facility's computer system, you should depend on which of the following factors?

1. The number of jobs to be scheduled
2. The system configuration only
3. The operating mode of the system only
4. The system configuration and operating mode

1-22. Which of the following is NOT an example of a computer operating mode?

1. Prime-time
2. Real-time
3. Online
4. Batch

1-23. As scheduler, you will be concerned with precomputer processing for which of the following reasons?

1. To see that the work is performed accurately
2. To see that sufficient magnetic media are available to store the data
3. To ensure that all inputs are received on time according to prearranged schedules
4. To ensure users are complying with standard operating procedures

1-24. If you schedule so much work for the computer that you overload the computer system, which of the following results is likely to occur?

1. AIS services are underutilized
2. User service deteriorates
3. Precomputer processing service deteriorates
4. Each of the above

1-25. As a scheduler, which of the following factors must you know about the files in use?

1. Where to find them in the magnetic media library
2. Where to store them in the magnetic media library
3. The record sizes and blocking factors of each file
4. How to reconstruct them

1-26. As a scheduler, what information must you know about the jobs you are to schedule?

1. How jobs interface only
2. How much time it takes to run each job only
3. How jobs interface and how much time it takes to run each job
4. How to operate the computer to back up production jobs

1-27. As a scheduler, you do NOT have to be proficient in which of the following skills?

1. Sound judgment
2. Tact and diplomacy
3. Analytical ability
4. Systems design

1-28. Production control acts as liaison between the AIS facility and the user community to perform which of the following functions?

1. Provide magnetic media support to the user
2. Provide programming services to the user
3. Adjust data flow and output schedules based on user and production requirements
4. Determine if errors are caused by hardware or systems/applications software

1-29. What functional area receives incoming work and checks to be sure the amount of input data is approximately the amount indicated on the production schedule?

1. Technical support
2. Quality control
3. I/O control
4. Data entry

1-30. Source documents are received and processed by what (a) functional area, and checked for completeness and accuracy by what (b) functional area?

1. (a) Data entry
   (b) Quality control
2. (a) Data entry
   (b) Technical support
3. (a) Scheduling
   (b) Quality control
4. (a) Scheduling
   (b) Technical support

1-31. To chart the interaction between the functional areas of an AIS facility, what type of chart should you prepare?

1. Data flowchart
2. Systems flowchart
3. Workload diagram
4. Workflow diagram

1-32. To determine what the demands will be on the AIS facility for the upcoming month, which of the following personnel usually meet(s) with the users?

1. Division chief only
2. Division chief and LPO only
3. Division chief, LPO, and scheduler
4. Computer operations supervisor and scheduler

1-33. During the forecasting phase of scheduling, you must remember to set aside time in the schedule for which of the following maintenance tasks?

1. File and computer
2. Tape drive
3. Disk drive
4. Each of the above

1-34. When you schedule recurring (old) jobs, which of the following types of information is/are best to use?

1. New estimates from users
2. Job experience and history
3. Latest job run time on your system
4. Average job run time on other systems

1-35. Scheduling enables management to make which of the following judgments?

1. A prediction of the effects of an increased workload
2. An evaluation of data entry operator skills
3. An analysis of production program errors
4. A plan for user training

1-36. As scheduler, you will need a backup or contingency plan for which of the following reasons?

1. To allow for hardware breakdowns and malfunctions
2. To schedule users' requirements
3. To allow for late submission of input from the user
4. To correct job parameters that are entered into the system incorrectly

1-37. Resource requirements, processing time, job dependencies, priorities, and deadlines are all what type of information?

1. Job-related
2. Workload-related
3. Resource-related
4. AIS facility-related

1-38. As scheduler, in addition to having information about computer resources, you need information about what other area(s) of processing?

1. Precomputer processing only
2. Postcomputer processing only
3. Precomputer and postcomputer processing
4. Output processing by users

1-39. What is the primary difficulty of manually scheduling jobs in a multiprogramming environment?

1. Specifying priorities
2. Specifying deadlines
3. Obtaining a job mix that handles job dependencies without processing jobs out of order
4. Obtaining a job mix that makes the best use of most resources without bogging down the entire computer system

2-40. Resources, workflow, system capabilities and capacities, and workload demands are all what type of information?

1. Job-related
2. Workload-related
3. Resource-related
4. AIS facility-related

1-41. To be sure sufficient time is scheduled for a job, you will probably want to add extra time to the estimated time as a safety factor. What is this type of time called?

1. Excess time
2. Time-plus
3. Real time
4. Buffer time

1-42. As scheduler, to provide for priority changes, special job requests, power outages, and corrective maintenance, you must take which of the following actions?

1. Reboot the computer system quickly without operator assistance
2. Readjust schedules quickly with a minimum of disruption
3. Revise your normal scheduling procedures to avoid these problems
4. Request scheduling assistance from computer operations personnel

1-43. When preparing a monthly schedule, you should be sure to include time for which of the following requirements?

1. Testing only
2. Planned maintenance only
3. Backup procedures only
4. Testing, planned maintenance, and backup procedures

1-44. Which of the following things do NOT normally affect the approved monthly schedule?

1. System backups
2. Software testing
3. System/program errors
4. Input files not available

1-45. A work load schedule is which of the following types of schedules?

1. External only
2. Internal only
3. External and internal

1-46. During production processing, monitoring the jobs to see that the work is being accomplished as planned is the responsibility of all except which of the following personnel?

1. Operator
2. I/O control clerk
3. Technical administrator
4. Production control coordinator

1-47. Who is the most qualified and highly trained individual to assist online users with their particular processing problems?

1. Operator
2. Shift supervisor
3. Production control clerk
4. Subsystem coordinator

1-48. Which of the following problems is one of the most frequent hardware problems associated with production processing?

1. Loss of power
2. Printer out of paper
3. Tape read/write errors
4. Wrong printer forms loaded

1-49. Which of the following problems is NOT a common external environmental problem?

1. Head crash
2. Loss of power
3. Voltage spikes
4. Loss of air conditioning

1-50. To correct software related problems, the operator must refer to which of the following sources for the corrective action to take?

1. Program operator manual only
2. Job run folder only
3. Program operator manual and job run folder
4. System manual

1-51. Unscheduled downtime can result from all except which of the following causes?

1. Power failures
2. Rebooting the system
3. Loss of air conditioning
4. System saves

1-52. When a software problem is researched, which of the following items is the most important?

1. Abort code
2. Program step
3. Action taken
4. Date job submitted

1-53. To improve performance and operation, you should provide feedback to all but which of the following people?

1. Shift supervisor
2. I/O control clerk
3. Technical administrator
4. Production control coordinator

1-54. To improve system performance, you can look for trends in the production process. Which of the following trends would NOT be looked at?

1. Impact of modified applications
2. Times when system was idle
3. Backlog of jobs to be run
4. Times when system seems slow

1-55. The amount of information you include in an AIS report should NOT exceed whose requirements?

1. User’s
2. Supervisor’s
3. Facility manager’s
4. Upper management’s

1-55. Which of the following items is NOT required in an ASDP?

1. Outline of the need
2. Prediction of the future need
3. Summary of the selected FIP resource solution
4. Summary of the projected costs

1-57. Downtime reported on the hardware utilization report includes which of the following types of downtime?

1. Whole system only
2. Each piece of equipment only
3. Whole system and each piece of equipment as appropriate
4. Equipment awaiting installation

1-58. Hardware under-utilization can be measured by excessive idle time.

1. True
2. False

1-59. Which of the following situations is NOT usually a cause of application software aborts?

1. File corrupted
2. File not available
3. Job run in sequence
4. Out of free disk space

1-60. Which of the following reports are good sources for determining what performance-tuning techniques to implement?

1. Hardware and software projection
2. Application software performance
3. Hardware utilization
4. Operating system software

1-61. With average program mixes, cache memory can-yield what percent increase in processing speed?

1. 30%
2. 40%
3. 50%
4. 60%

1-62. You can make all but which of the following changes to the operating system?

1. Change memory addresses
2. Reconfigure disk drives
3. Reconfigure the system
4. Change buffer sizes

1-63. When submitting a trouble report, you must follow the instruction from which of the following commands?

1. The type commander
2. The command receiving the trouble report
3. The command sending the trouble report

1-64. When you cannot work around a problem to continue operating, what priority should you assign to the trouble report?

1. Critical
2. Routine
3. Urgent

1-65. When you can work around the problem but a resolution is required immediately, what priority should you assign to the trouble report?

1. Critical
2. Routine
3. Urgent

1-66. All of the following are common reasons for the submission of a hardware trouble report except which one?

1. System keeps locking up
2. System keeps dropping I/O channels
3. Corrupted file and no save tapes are available
4. Bad data entered in file

l-67. When preparing the operational guidelines for your facility, which of the following areas should you consider?

1. Backup operations only
2. Contingency plans and disaster recoveries only
3. Emergency responses only
4. Backup operations, contingency plans and disaster recoveries, and emergency responses

1-68. Which of the following is NOT a common reason for urgent change requests?

1. Changes to the operating system
2. Equipment degradation
3. System testing
4. Special saves

ASSIGNMENT 2

Textbook Assignment: "Communications Administration," chapter 2, pages 2-1 through 2-29.

2-1. DCS circuits are owned or leased by what organization?

1. AT&T
2. The Joint Military Communications Management Office
3. The U.S. Government
4. NAVCOMTELCOM

2-2. The DCS combines elements from the three military services into a single communications system.

1. True
2. False

2-3. Who exercises operational control over the DCS?

1. The civilian head of the DCA
2. The head of the JCS
3. The military head of the NTS
4. The military head of DISA

2-4. What is the mission of naval communications?

1. To provide reliable, secure, and rapid communications
2. To provide reliable, simple, and rapid communications
3. To provide controlled, secure, and functional communications
4. To provide easy, secure, and rapid communications

2-5. Naval communications includes which of the following policies?

1. To promote the safety of life at sea and in the air by maintaining communications with appropriate communications facilities
2. To encourage at all levels of command an effort to improve techniques, procedures, and efficiency
3. To establish and maintain effective communications within the Department of the Navy
4. Each of the above

2-6. Concerning area of coverage, what is the primary distinction between the NTS and the DCS?

1. The DCS units are fleet associated, and the NTS facilities are primarily ashore
2. The NTS facilities are fleet associated, and the DCS units are primarily ashore
3. Navy teleprinter communications are within the realm of the NTS; Navy communications by any other means are under the cognizance of the DCS
4. Navy teleprinter communications are within the realm of the DCS; Navy communications by any other means are under the cognizance of the NTS

2-7. Who is responsible for operational and management control of the elements of the NTS?

1. Commander, Naval Support Force
2. Commander, Naval Computer and Telecommunications Command
3. Commander in Chief, Atlantic Fleet
4. Chief of Naval Operations

2-8. How do fleet commanders assign communications responsibilities to their respective fleets?

1. Communications Information Bulletins (CIBs)
2. Wide Area Network (WAN)
3. Operation Orders (OPORDs)
4. Naval messages

2-9. The world is divided into what total number of Nava] Communications Areas (NAVCOMMAREAS)?

1. Five
2. Six
3. Three
4. Four

2-10. Who exercises coordination and control of all naval communications within each NAVCOMMAREA?

1. Officer in Charge, NAVCOMMAREA
2. Naval Computer and Telecommunications Area Master Station
3. The fleet CINC in the area
4. Naval Communications Station

A. NCTAMS
B. NAVCOMTELSTA
C. NAVCOMTELDET
D. NAVSECGRUDEPT

Figure 2A

IN ANSWERING QUESTIONS 2-11 THROUGH 2-14, SELECT FROM FIGURE 2A THE NAVAL TELECOMMUNICATIONS COMMAND ELEMENT DESCRIBED.

2-11. Assigned a limited or specialized mission.

1. A
2. B
3. C
4. D

2-12. Responsible for cryptologic operations.

1. A
2. B
3. C
4. D

2-13. Entry point for Navy Tactical Satellite Systems.

1. A
2. B
3. C
4. D

2-14. Provides Naval Industrial Fund ADP services.

1. A
2. B
3. C
4. D

2-15. When you are assigned as a communications manager, what should be your first consideration?

1. Compare the communications organization with others of similar size
2. Evaluate the effectiveness of organization' s communications
3. Evaluate the personnel training program
4. Rotate personnel in their jobs to improve training

2-16. To measure the effectiveness of the operations and services-provided by your communications facility, you should establish standards of performance for which of the following areas?

1. Speed
2. Security
3. Reliability
4. A1l of the above

2-17. Fixed standards for work measurement processes present what potential problem?

1. They may prevent changes that are needed as a result of changing conditions
2. They limit variety in work assignments
3. They tend to limit individual work potential
4. They allow for individual initiative, which is undesirable

2-18. To overcome resistance to changes in performance standards, which of the following methods is recommended?

1. Show the personnel concerned how wasteful their former methods were
2. Give personnel a complete description of the changes being made
3. Permit personnel who will be-affected by the changes to participate in the organizing effort
4. Advise the personnel concerned that they must overcome their natural resistance to change

2-19. You may improve overall personnel performance by evaluating which of the following factors?

1. Personnel requirements
2. Existing organizational structure
3. Both 1 and 2 above
4. The need for qualified replacements

2-20. A lack of efficiency in a communications division is a direct reflection of the management skills of which of the following individuals?

1. Commanding officer
2. Senior supervisor
3. Training officer
4. Watchstanders

2-21. To reorganize divisional workflow and workspace layout, what information do you need to plan properly?

1. What work is to be done
2. When the work is to be performed
3. HOW the work is to be accomplished
4. Each of the above

2-22. What is a major responsibility of a supervisor?

1. Promote timeliness
2. Monitor production
3. Maintain proper work hours
4. Ensure personnel are fit

2-23. When office layout is being planned, what is the primary consideration?

1. Security of classified material
2. Safety factors
3. Number of personnel to be accommodated
4. Proper flow of paper and work

2-24. The physical layout of your office should be arranged so that paperwork will flow in what direction(s)?

1. One direction
2. A clockwise direction
3. Back-and-forth
4. Two directions at once

2-25. What publication lists the types of ships that are required to have a communications department?

1. NWP 1 (NWP 2-01)
2. ACP 100
3. NWP 4 (NWP 6-01)
4. NTP 4

2-26. Who is responsible to the communications officer for compliance with communications directives and for the accurate and rapid handling of messages?

1. Communications watch officer
2. Senior watch supervisor
3. Communications center supervisor
4. Technical control supervisor

2-27. Who directly supervises all radiomen on watch in the message processing area and is responsible for notifying the CWO and SWS on any unusual or urgent matters?

1. Assistant watch supervisor
2. Radio officer
3. Communications center supervisor
4. Technical control supervisor

2-28. Who is responsible for examining operational logs, monitoring equipment alignment and operation, and preventing message backlogs?

1. Communications center supervisor
2. Senior watch supervisor
3. Radio officer
4. Technical control supervisor

2-29. Who has full responsibility for the internal handling of message traffic within the ship?

1. Commanding officer
2. Executive’ officer
3. Communications officer
4. Radio officer

2-30. Who is responsible for the organization, supervision, and coordination of the command's external communications?

1. Radio officer
2. Communications officer
3. Communications watch officer
4. Communications watch. supervisor

2-31. Who is responsible for preparing and maintaining the communications watch, quarter, and station bill?

1. Communications officer
2. Communications watch officer
3. Radio officer
4. Senior watch supervisor

2-32. Who is responsible for maintaining the status board which displays equipment, nets, and circuit information?

1. Communications officer
2. Communications center supervisor
3. Senior watch supervisor
4. Technical control supervisor

2-33. Who is responsible for managing the command's CMS account and for advising the commanding officer on all matters concerning CMS?

1. Communications officer
2. Radio officer
3. Crypto officer
4. CMS officer

2-34. Directives issued by naval commanders to effect the coordinated execution of an operation are known by what term?

1. Communications plan (COMMPLAN)
2. Execution order (EXORD)
3. operation order (OPORD)
4. Standard operating procedure (SOP)

2-35. An OPORD is made up of what three parts?

1. Heading, plan, and closure
2. Beqinning, body, and annex
3. Heading, body, and closure
4. Heading, body, and ending

2-36. Detailed information for various ship departments is contained in what two enclosures?

1. Annexes and appendices
2. Annexes and tabs
3. Appendices and indexes
4. Annexes and indexes

2-37. A document issued by an organization to advise its personnel of internal routine practices is most commonly issued in what format?

1. Division instruction
2. Division officer instruction
3. Standard operating procedure
4. Operational instruction

2-38. How detailed a standard operating procedure (SOP) is depends on which of the following factors?

1. The state of training
2. The complexity of the instructions
3. The size of the command
4. Each of the above

4-39. What type of message is destined for two or more addressees, none of whom is informed of any other addressee?

1. Book
2. General
3. Multiple-address
4. Single-address

4-40. What type of message has a wide, predetermined, standard distribution?

1. Book
2. General
3. Multiple-address
4. Single-address

2-41. How can four-letter address groups be distinguished from Navy four-letter international radio call signs?

1. Address groups are transmitted with a hyphen between the first and second letters
2. Address groups are transmitted with a hyphen between the third and fourth letters
3. Address groups are always transmitted twice
4. Address groups do not begin with the letter N

4-42. What type of address group must always have more information added to it to serve as a complete station and address designator?

1. Individual activity address group
2. Collective address group
3. Conjunctive address group
4. Address indicating group

4-43. What always precedes geographic address groups?

1. Individual activity address groups
2. Collective address groups
3. Conjunctive address groups
4. Address indicating groups

4-44. What is the purpose of address indicating groups (AIGs)?

1. To reduce the number of address groups required in the heading of a message
2. To convey special instructions in the heading of a message
3. To provide an alternate address group in the event that the primary address group is compromised
4. To locate the originator of a message geographically

4-45. A single address group that represents a set of four or more activities, including the cognizant authority, is known by what term?

1. Conjunctive address group
2. Collective address group
3. Collective address desiqnator
4. Call-sign

2-46. The Navy uses GMT as a common 24-hour worldwide time standard in messages for the date-time group and time of file. What does GMT stand for?

1. Greenwich Mean Time
2. General Master Time
3. Greenwich Master Time
4. Global Mean Time

2-47. The world is divided into what total number of GMT time zones?

1. 6
2. 12
3. 24
4. 48

2-48. The time zone which passes through Greenwich, England, is most commonly known by what term?

1. GREEN time zone
2. ROMEO time zone
3. YANKEE time zone
4. ZULU time zone

2-49. If you were stationed in time zone ROMEO, how would you convert (a) local time to GMT and (b) GMT to local time?

1. (a) Subtract 5 hours from local time
   (b) add 5 hours to GMT
2. (a) Add 5 hours to local time
   (b) subtract 5 hours from GMT
3. (a) Subtract 5 hours from GMT
   (b) add 5 hours to local time
4. (a) Add 5 hours to GMT.
   (b) subtract 5 hours from local time

2-50. An eastbound ship crossing the international date line loses a day.

1. True
2. False

2-51. What is an important point to remember about the MIKE and YANKEE zones?

1. The day changes along with the time, plus or minus 1 hour
2. The day remains the same, but the time changes, plus or minus 1 hour
3. The day and the time remain the same
4. The day changes, but the time remains the same

2-52. How many digits make up the Julian date?

1. Nine
2. Seven
3. Six
4. Four

2-53. The precedence of a message should be based on what factor?

1. The urgency of the message
2. The classification of the message
3. The number of addressees who are to receive the message
4. The importance of the subject matter

2-54. What is the highest precedence that is normally authorized for administrative messages?

1. Routine
2. Priority
3. Immediate
4. Flash

2-55. What precedence is assigned to a message that is of such urgency that it must be brief?

1. Priority
2. Immediate
3. Yankee
4. Flash

2-56. What precedence is limited to designated emergency action command and control messages within the AUTODIN system?

1. Priority
2. Immediate
3. Flash
4. Yankee

2-57. Composing a message and selecting the proper classification and precedence is the responsibility of what individual?

1. The drafter
2. The releaser
3. The originator
4. The commanding officer

2-58. Before accepting a message originated in or destined for an area under minimize for transmission, the outrouter must ensure that which of the following information is on the message?

1. The notation “MINIMIZE CONSIDERED” in the appropriate area of the message form
2. The releaser’s name and rank/grade in the last line of the message text
3. Both 1 and 2 above
4. The notation “MINIMIZE CONSIDERED” stamped on the message form or diskette

2-59. Which of the following messages are used to determine delay or nondelivery of a message on a station-to-station basis?

1. Pro forma
2. Service only
3. Tracer only
4. Both service and tracer

2-60. Which of the following messages are described as short and concise messages between operators dealing with message corrections, broadcast reruns, and missent or misrouted messages?

1. Pro forma
2. MINIMIZE
3. Service only
4. Service and tracer

2-61. Where does an activity send the results of a tracer investigation?

1. To the originator of the tracer message only
2. To the preceding station(s) only
3. To the originator of the tracer message and the preceding station(s) only
4. To the originator of the tracer message, the preceding station(s), and the following station

2-62. To establish a termination with a NCTAMS or NAVCOMTELSTA, a ship must send a request what minimum time in advance?

1. 24 hr
2. 48 hr
3. 72 hr
4. 96 hr

2-63. When it needs to shift broadcast guard, a ship sends what type of message?

1. Termination request message
2. Communications guard shift
3. Service message
4. Broadcast screen request

2-64. Broadcast screen requests should be sent to what organization?

1. Broadcast rerun station
2. Broadcast radiating station
3. Broadcast control station
4. Broadcast keying station

2-65. A COMMSPOT report should be sent under what circumstances?

1. As soon as unusual communication difficulties arise
2. As soon as communication difficulties are corrected
3. Whenever unusual communication difficulties are expected
4. Durinq solar flare-ups

2-66. What type of message is placed in the cryptocenter file?

1. SPECAT
2. SPECAT SIOP-ESI
3. TICON
4. NATO

A. Authentication

B. Codes

C. Ciphers

D. Radio silence

E. Monitoring

F. Identification Friend or Foe (IFF)

Figure 2A

IN ANSWERING QUESTIONS 2-67 THROUGH 2-72,SELECT THE SECURITY DEVICE OR PROCEDURE FROM FIGURE 2A THAT IS BEST DESCRIBED IN THE QUESTION.

2-67. Any cryptologic system in which arbitrary symbols or groups of symbols represent units of plain text.

1. A
2. C
3. E
4. F

2-68. Uses electromagnetic transmissions to which equipment carried by friendly forces automatically respond.

1. B
2. C
3. E
4. F

2-69. A procedure designed to protect communications systems against acceptance of false transmissions or simulations by establishing the validity of a transmission, message, or originator.

1. A
2. B
3. C
4. D

2-70. A system of communication in which arbitrary groups of symbols represent units of plain text; used for brevity and/or security.

1. A
2. B
3. C
4. E

2-71. A condition in which all or certain radio equipment is kept inoperative.

1. A
2. B
3. C
4. D

2-72. The act of listening, carrying out surveillance on, and/or recording the emissions of own or allied forces.

1. A
2. B
3. E
4. F

2-73. The communications plan satisfies communications requirements by providing what information?

1. Specifies circuit operators, equipment, and traffic capabilities
2. Establishes watchbills, software requirements, and deployment times
3. Designates enemy communications frequencies, supporting COMMSTAs, and supply requirements
4. Specifies circuits, channels, and facilities to be used

2-74. What document initiates the addition, deletion, or change to an existing DCS circuit?

1. Telecommunications Service Order (TSO)
2. Telecommunications Service Request (TSR)
3. Circuit Service Transfer (CST)
4. Request for Modification of Circuit (RMC)

ASSIGNMENT 3

Textbook Assignment: "Communications Administration (continued)," chapter 2, pages 2-29 through 2-37; "Communications, Security," chapter 3, pages 3-1 through 3-12; "AIS Security," chapter 4, pages 4-1 through 4-12.

3-1. If you desire to delete an existing DCS circuit, you should submit what type of request?

1. An AUTODIN deletion request
2. A telecommunications service request
3. A DCA circular request
4. A technical control service request

3-2. Requirements for new telecommunications services should be defined and submitted what minimum time in advance?

1. 1 yr
2. 2 yr
3. 3 yr
4. 6 mo

3-3. What does a TSO authorize?

1. Funding to begin basic circuit design
2. Starting, changing, or discontinuing circuits
3. Procurement of specific devices or ancillary equipment
4. Both 2 and 3 above

3-4. Navy funds cannot be obligated for developing or procuring communications equipment that uses a portion of the frequency spectrum until what is obtained?

1. Frequency usage estimate
2. A frequency allocation
3. A spectrum study
4. An FCC recommendation

3-5. Which of the following constraints should be considered when a frequency assignment is authorized?

1. Power, emission bandwidth, location of antennas, and operating time
2. Power, receiver locations, and atmospheric conditions
3. Bandwidth, sidebands, harmonics, and power requirements
4. Power, harmonics, and RF hazards to personnel

3-6. What authority grants Navy and Marine Corps activities within the U.S. permission to use radio frequencies?

1. Naval Electromagnetic Spectrum Center (NAVEMSCEN)
2. National Telecommunications and Information Administration (NTIA)
3. United States Military Communications Electronics Board (USMCEB)
4. Chief of Naval Operations (CNO)

3-7. In the Navy, what organization authorizes frequency assignment applications?

1. The United States Military Communications Electronics Board (USMCEB)
2. The National Telecommunications and Information Administration (NTIA)
3. The Joint Chiefs of Staff
4. The Naval Electromagnetic Spectrum Center (NAVEMSCEN)

3-8. Who is authorized to send PERSONAL FOR messages?

1. E-7 military or GS-7 civilian (or above)
2. Officers of flag rank or in a command status only
3. All officers
4. Anyone who needs to send a personal message

3-9. What is contained in the publications in the NWPL?

1. Manning plans, battle organizations, and future deployment schedules
2. Awards information, maintenance schedules, and supply information
3. Required procedures, signals, and other operational and mission-essential information
4. Operational requirements, battle organizations, and deployment schedules

3-10. What is the objective of the central administration of the NWPL?

1. To ensure that the publications in the NWPL are correct and readily avail-able for use
2. To ensure that personnel have a place to study for advancement
3. To ensure that personnel have access to publications and periodicals on the latest technology
4. To ensure that personnel have access to the most recent and best-selling novels

3-11. Who is responsible for the management of the NWPL?

1. The naval warfare publications officer
2. The naval warfare publications custodian
3. The naval warfare publications librarian
4. The naval warfare publications manager

3-12. What publication provides guidance for the administration and security of the NWPL?

1. OPNAVINST 5510.1
2. NTP 4
3. NWP 4 (NWP 6-01)
4. NWP 0 (NWP 1-01)

3-13 . Who is responsible for changes or corrections to NWPL publications?

1. The NWPL clerk
2. The primary user
3. The NWPL custodian
4. The communications watch officer

3-14. Who is considered to be a holder under the administration of NWPL?

1. A person who holds NWPL publications for short terms only
2. A person who transports publications to and from the NWPL
3. A person who has permanent subcustody of publications from the NWPL
4. The NWPL custodian

3-15. Which of the following files are used in NWPL maintenance?

1. Signature and custody fries
2. Administrative and transaction files
3. Signature and administrative files
4. Custody and administrative files

3-16. The NWPL administrative file is also known by what other term?

1. Transaction file
2. Office file
3. A-1 file
4. Custody file

3-17. Material in the administrative file must be retained for what minimum time ?

1. 1 yr
2. 2 yr
3. 5 yr
4. 6 mo

3-18. What colors are assigned to the binders for U.S. naval warfare publications of different classifications?

1. Secret - red, Confidential - green, Unclassified - white
2. Secret - red, Confidential - yellow, Unclassified - blue
3. Secret - red, Confidential - yellow, Unclassified - white
4. Secret - red, Confidential - green, Unclassified - blue

3-19. Where is the effective date of the publication change/correction found?

1. In the Record of Changes page
2. In the List of Effective Pages (LOEP)
3. In the Foreword or Letter of Promulgation
4. In the Title page

3-20. Which of the following colors should be used to make pen-and-ink corrections to NWPL publications?

1. Green only
2. Black or blue only
3. Any dark color except red
4. Any color is acceptable

3-21. What does the designation "NMC 6/2" on a correction mean?

1. It is the 6th message correction and will-be incorporated into the publication by printed change number 2
2. It is the 2nd message correction and will be incorporated into the publication by printed change number 6
3. It was sent on the 2nd of June of the current year
4. It is the 6th change to the 2nd revision of the publication

3-22. What document contains guidance for taking extracts from a NATO publication?

1. OPNAVINST 5510.1
2. ACP 121
3. NWP 0 (NWP 1-01)
4. NATO letter of promulgation

A. ACPs
B. NTPs
C. JANAPs
D. NWPs

Figure 3A

IN ANSWERING QUESTIONS 3-23 THROUGH 3-26, SELECT THE PUBLICATIONS FROM FIGURE 3A THAT ARE DESCRIBED.

3-23. Provide communications instructions and procedures essential to conducting combined military operations in which two or more allied nations are involved.

1. A
2. B
3. C
4. D

3-24. Coordinate and standardize communications procedures among U.S. military services.

1. A
2. B
3. C
4. D

3-25. Main publications used by Navy, Coast Guard, and Marine personnel for communications.

1. A
2. B
3. C
4. D

3-26. Incorporate the results of fleet tactical development and evaluation programs and NATO experience and provide information about the tactical capabilities and limitations of equipment and systems.

1. A
2. B
3. C
4. D

A. CMS account
B. CMS custodian
C. CMS local holder
D. CMS user

Figure 3B

IN ANSWERING QUESTIONS 3-27 THROUGH 3-29, SELECT THE TERM FROM FIGURE 3B THAT IS DESCRIBED.

3-27. A command with an account number that draws its COMSEC material directly from national or Navy distribution sources.

1. A
2. B
3. C
4. D

3-28. COMSEC material needs are met by drawing such material from the squadron commander.

1. A
2. B
3. C
4. D

3-29. An individual who requires the use of COMSEC material for a short time to accomplish a specific task.

1. A
2. B
3. C
4. D

3-30. Which of the following statements concerning storage requirements for COMSEC material is/are correct?

1. COMSEC material may be stored with other communications material according to security classification
2. COMSEC material must be stored separately from non-COMSEC material
3. COMSEC material of different classification may be stored. together regardless of classification if storage limitations are a factor
4. Both 2 and 3 above

3-31. What number of signatures is/are required on the COMSEC watch-to-watch inventory sheet?

1. One
2. Two
3. Three
4. Four

3-32. What is the maximum length of time that you are authorized to hold superseded (a) keying material marked CRYPTO and (b) authentication publications?

1. (a) 24 hours (b) 24 hours
2. (a) 12 hours (b) 5 days
3. (a) 5 days (b) 12 hours
4. (a) 5 days (b) 5 days

3-33. What are the three types of keying material in descending priority of destruction?

1. Superseded, reserve, effective
2. Effective, superseded, reserve
3. Reserve, effective, superseded
4. Superseded, effective, reserve

3-34. Effective keying material is the most sensitive of the three types of keying material.

1. True
2. False

3-35. What is the purpose of Two-Person Integrity?

1. To prevent a single person from having access to COMSEC material
2. To prevent more than two persons from having access to COMSEC material
3. To provide for an alternate custodian in the event the primary is unavailable
4. To allow for a division of responsibilities among the custodians

A. CRYPTO
B. Cryptoinformation
C. Crypto-related information
D. Cryptosystem

Figure 3C

IN ANSWERING QUESTIONS 3-36 THROUGH 3-39, SELECT THE TERM FROM FIGURE 3C THAT IS DESCRIBED.

3-36. Marking used to protect or authenticate national security-related information on all keying material and associated equipment.

1. A
2. B
3. C
4. D

3-37. Always classified and normally concerns the encryption or decryption process of a cryptosystem.

1. A
2. B
3. C
4. D

3-38. May be classified or unclassified; normally associated with cryptomaterial but not significantly descriptive of it.

1. A
2. B
3. C
4. D

3-39. Encompasses all associated items of cryptomaterial that provide a single means of encryption and decryption.

1. A
2. B
3. C
4. D

3-40. A failure that adversely affects the security of a cryptosystem is known by what term?

1. Cryptoexposure
2. Cryptoinstability
3. Cryptodeficiency
4. Cryptoinsecurity

3-41. A system within a general system confined to actual encryption, decryption, or authentication is known by what term?

1. Cryptovariable
2. Specific cryptosystem
3. Secondary cryptosystem
4. Supporting cryptosystem

3-42. The most frequently changed element of a cryptosystem is known by what term?

1. Primary cryptovariable
2. Secondary cryptovariable
3. Crypto modifier
4. Cryptosystem internal variable

3-43. What are the primary advantages of (a) over-the-air rekey (OTAR) and (b) over-the-air transfer (OTAT)?

1. (a) Requires less circuit downtime for loading keylists, and (b) no operator training required
2. (a) Reduces distribution of physical keying material, and (b) eliminates process of loading equipment with key tapes
3. (a) Reduces distribution of physical keying material, and (b) no operator training required
4. (a) Eliminates process of loading equipment with key tapes, and (b) no operator training required

3-44. What is the purpose of transmission authentication?

1. To guard against fraudulent or simulated transmissions
2. To inform the other operator that you are receiving the transmission
3. To acknowledge the transmission of the other operator
4. To allow the other operator to acknowledge your transmission

3-45. The self-authentication method is used in which of the following transmissions?

1. Transmission and reply
2. Challenge and reply
3. Transmission authentication
4. Challenge authentication

3-46. When you receive a message that has an authenticator in it, what action, if any, are you required to take?

1. Prepare a message to challenge the originator
2. Send a message that you are in receipt of the message
3. Pass the message on to higher authority for them to challenge the originator
4. None

3-47. As an operator, you are required to authenticate in which of the following situations?

1. You suspect intrusion on the circuit
2. You are requested to authenticate
3. You are requested to break radio silence
4. Each of the above

A. Meaconing
B. Interference
C. Jamming
D. Intrusion

Figure 3D

IN ANSWERING QUESTIONS 3-48 THROUGH 3-51, SELECT THE TERM FROM FIGURE 3D THAT IS DEFINED.

3-48. The interception and rebroadcast of navigational signals on the same frequency.

1. A
2. B
3. C
4. D

3-49. An attempt by the enemy to enter U.S. or allied communications systems and simulate traffic with the intent to confuse and deceive.

1. A
2. B
3. C
4. D

3-50. The deliberate use of electromagnetic signals with the objective of impairing communications circuits.

1. A
2. B
3. C
4. D

3-51. Usually a nondeliberate electrical disturbance that unintentionally prevents the effective use of a frequency.

1. A
2. B
3. C
4. D

3-52. Which of the following statements best describes the overall goal of AIS security?

1. To take all reasonable measures to protect AIS assets
2. To prevent data and programs from being destroyed or sabotaged
3. To keep unauthorized personnel out of your AIS facility
4. To take whatever measures are necessary to protect equipment and people

3-53. Which of the following assets is NOT considered an AIS asset?

1. People
2. Hardware
3. Software
4. Environment

3-54. In AIS security terminology, what term is used for the things that can destroy AIS assets?

1. Threats
2. Probability
3. Vulnerability
4. Countermeasures

3-55. To express the cost of a loss or abuse from an adverse event over time, what AIS security term is used?

1. Risk
2. Likelihood
3. Vulnerability
4. Countermeasure

3-56. In AIS security, risks are usually expressed in which of the following terms?

1. Days
2. Dollars
3. Equipment
4. Personnel

3-57. In AIS security terminology, the controls to lessen or eliminate known threats and vulnerabilities are called

1. physical barriers
2. security routines
3. backup procedures
4. countermeasures

3-58. Under AIS security, countermeasures (controls) that are embedded in hardware, software, and telecommunications equipment are what type of controls?

1. Physical
2. Technical
3. Managerial
4. Administrative

3-59. Under AIS security, countermeasures (controls) that concern people and procedures, such as who is authorized to do what or who receives or requests a sensitive report, are what type of controls?

1. Physical
2. Technical
3. Managerial
4. Administrative

3-60. Under AIS security, countermeasures (controls) that concern planning and evaluation, such as audits to review the effectiveness and efficiency of countermeasures that are in place, are what type of controls?

1. Physical
2. Technical
3. Managerial
4. Procedural

3-61. In regard to AIS security, the continuation of an activity's mission during abnormal operating conditions is provided by which of the following means?

1. Countermeasures
2. Contingency plans
3. Security risk plan
4. Emergency response team

3-62. In addition to hardware and software, what are the other three areas of consideration for the Navy's AIS security program?

1. Data, personnel, and environment
2. Data, human resources, and logistics
3. Data, human resources, and communications
4. Media libraries, environment, and communications

3-63. Which of the following personnel serves as the single point of contact for all matters related to AIS security?

1. Executive officer
2. Information system security manager
3. Security violations officer
4. Systems security manager

3-64. AIS security is not really that difficult to understand. What percent is (a) common sense, and (b) proper training?

1. (a) 55% (b) 45%
2. (a) 60% (b) 40%
3. (a) 65% (b) 35%
4. (a) 70% (b) 30%

3-65. The manufacturer's optimum temperature and humidity range specifications for AIS equipment operation are NOT available. Which of the following (a) temperature and (b) humidity ranges are considered acceptable for computer operation?

1. (a) 65° ±5° (b) 55% ±5%
2. (a) 65° ±5° (b) 65% ±2%
3. (a) 72° ±2° (b) 55% ±5%
4. (a) 72° ±2° (b) 65% ±2%

3-66. In AIS environmental security, emergency lights are installed in computer facilities for what primary reason?

1. To protect personnel
2. To assist fire fighters
3. To locate AIS equipment
4. To locate fire-fighting equipment

3-67. Fluctuations in electrical power can adversely affect the operation of AIS equipment. If your command's mission dictates continuous AIS support, each computer system should be equipped with which of the following equipment?

1. A motor/generator
2. An ac, dc regulator
3. A voltage surge protector
4. An uninterrupted power source

3-68. In regard to AIS security, master control switches are used to shut off all power to your AIS spaces in the event of a fire. These master control switches are normally installed at what location?

1. In the CO^2 storage room
2. In the security officer's space
3. At the exit doors of the AIS spaces
4. On the master control panel of the computer

3-69. Which of the following security modes does NOT apply to processing classified or level I data?

1. Dedicated
2. System low
3. Multilevel
4. System high

3-70. For processing classified, the central computer facility and all its related peripheral devices (both local and remote) are protected for the highest classification category and type of material contained in the system. The system is said to be in what security mode?

1. Controlled
2. System low
3. System high
4. Totally dedicated

3-71. For processing level I data, the central computer facility and all its related peripheral devices (both local and remote) are exclusively used and controlled by specific users having a security clearance and need-to-know for the processing of a particular cateqory of classified material. The system is operating in what security mode?

1. Dedicated
2. System low
3. Multilevel
4. System high

3-72. For processing level I data, an AIS system provides the capability of permitting various categories of classified materials to be stored, processed, and selectively accessed on a concurrent basis by users having differing clearances and need-to-know. The system is said to be in what security mode?

1. Controlled
2. Undedicated
3. System low
4. Multilevel

3-73. What category of AIS media is considered temporary in nature and is retained for 180 days or less?

1. Smooth
2. Working
3. Finished
4. Intermediate

3-74. Which of the following categories of AIS media is permanent in nature and is retained for a period of more than 180 days?

1. Smooth
2. Working
3. Finished
4. Intermediate

ASSIGNMENT 4

Textbook Assignment: "AIS Security (continued)," chapter 4, pages 4-13 through 4-26.

4-1. In which of the following steps in planning an AIS security program, will major problem areas be identified?

1. Perform action plans
2. Perform preliminary planning
3. Perform a preliminary risk analysis
4. Perform and document a detailed risk analysis

4-2. Which of the following steps in planning an AIS security program allows for review and approval?

1. Perform action plans
2. Perform preliminary planning
3. Perform a preliminary risk analysis
4. Perform and document a detailed risk analysis

4-3. A security policy statement should provide which of the following information?

1. General guidance and assignment of responsibilities
2. General guidance and listing of responsibilities
3. Detailed guidance and assignment of responsibilities
4. Detailed guidance and listing of responsibilities

4-4. As a guideline for risk analysis, which of the following FIPS publications should you use?

1. FIPS PUB 47
2. FIPS PUB 53
3. FIPS PUB 65
4. FIPS PUB 79

4-5. The impact of a given threat may depend on all but which of the following factors?

1. Geographical location
2. Local environment
3. Perceived threat of vandals
4. Potential value of property to a thief

4-6. Which of the following is a threat to an AIS facility?

1. Hardware failure
2. Tampering with inputs, programs, and data
3. Accidents causing nonavailability of key personnel
4. Each of the above

4-7. It is recommended that the AIS facility upper management begin development of the security program with a/an

1. risk analysis
2. inventory of equipment
3. survey of data integrity
4. intensive training program

4-8. A quantitative risk analysis produces which of the following results?

1. Long-range planners receiving guidance on personnel requirements
2. The security program objectives directly relating to the mission of the command
3. Criteria generated for designing and evaluating internal controls
4. An estimate of losses to be expected

4-9. When the risk analysis is prepared, the first step to be considered is to

1. develop an estimate of annual loss expectancy
2. estimate the potential losses to which the AIS facility is exposed
3. evaluate the threats to the AIS facility
4. review the security program objectives

4-10. The loss potential estimate has which of the following objectives?

1. To place a monetary value on the loss estimate only
2. To identify critical aspects of the AIS facility operation only
3. To place a monetary value on the loss estimate and to identify critical aspects of the AIS facility operation
4. To determine data replacement requirements

4-11. The loss of program files has which of the following loss potentials?

1. Cost to replace assets
2. Cost to reconstruct files
3. Security compromise
4. Value of assets stolen before loss is detected

4-12. Which of the following is the loss potential that may result from the indirect theft of assets?

1. Cost to replace assets
2. Cost to reconstruct files
3. Security compromise
4. Value of assets stolen before loss is detected

4-13. To show replacement costs for the physical assets of the AIS facility, AIS technical managers and upper management should use which of the following methods?

1. Build a graph
2. Construct a table
3. Produce a list
4. Write a description

4-14. The AIS technical manager should call on which of the fallowing personnel to assist in making loss estimates?

1. Users
2. Vendors
3. Programmers
4. Supervisors

4-15. After a preliminary screening to identify the critical tasks, the AIS technical manager should perform which of the following tasks next?

1. Determine the scope of the critical tasks
2. Develop an estimate of annual loss expectancy
3. Quantify loss potential with the help of user representatives
4. Determine the back-up system requirements for the critical tasks

4-16. The second step to be considered when you prepare the risk analysis is to

1. develop an estimate of annual loss expectancy
2. estimate the potential losses to which the AIS facility is exposed
3. evaluate the threats to the AIS facility
4. review the security program objectives

4-17. To develop estimates of the occurrence probability for each type of threat, the AIS technical manager should use all except which of the following resources?

1. Standardized Navy-wide formula
2. Higher authority instructions/manuals
3. Common sense
4. Data

4-18. The third step to be considered when you prepare the risk analysis is to

1. develop an estimate of annual loss expectancy
2. estimate the potential losses to which the AIS facility is exposed
3. evaluate the threats to the AIS facility
4. review the security program objectives

4-19. Fire, flood, and sabotage, in varying degrees, result in which of the following losses?

1. Indirect loss of assets
2. Physical destruction
3. Data compromise
4. Theft of information

4-20. Reducing the probability of some occurrence by altering the environment could be accomplished in which of the following ways?

1. Implementing more rigorous standards for programming and software testing
2. Preparing a backup system for offsite operations
3. Providing military guards and special door locks
4. Relocating the AIS facility

4-21 Which of the following is an example of erecting barriers to ward off a threat?

1. Implementing more rigorous standards for programming and software testing
2. Preparing a backup system for offsite operations
3. Providing military guards and special door locks
4. Relocating the AIS facility

4-22. When selecting a specific remedial measure, a total of how many criteria should be used?

1. One
2. Two
3. Three
4. Four

4-23. Which of the following is one possible way to select a remedial measure to minimize a threat?

1. Begin with the threat having the largest annual loss potential
2. Begin with only those measures for which the cost can be estimated precisely
3. Begin with only those remedial measures that would not cause a loss reduction in the same area
4. Begin with the remedial measures for which the annual cost is more than the expected reduction in annual loss

4-24. All but which of the following events tends to have the same basic effect as the others on AIS operations?

1. Fire
2. Rain
3. Earthquake
4. Windstorm

4-25. In minimizing an AIS building's exposure to fire damage, which of the following factors should be considered?

1. Contractors
2. Design only
3. Location only
4. Design and location

4-26. An AIS physical security program should include which of the following fire safety elements?

1. Measures to ensure prompt detection of and response to a fire emergency
2. Provision for quick human intervention and adequate means to extinguish fires
3. Provision of adequate means and personnel to limit damage and effect prompt recovery
4. All of the above

4-27. In evaluating the fire safety of an AIS facility, a total of how many factors are to be considered?

1. Five
2. Six
3. Three
4. Four

4-28. Which of the following factors affects the degree of hazard associated with a given occupancy?

1. Weight of the material
2. Amount of combustible material
3. Exposed surface of the material
4. Package in which the material is stored

4-29. When the safety features of an AIS facility building are designed, which of the following factors should be considered?

1. Heat-resistant lights
2. Building operation
3. Fire walls
4. Storm doors

4-30. The inherent fire safety of a building can be rendered ineffective because of which of the following conditions?

1. Fire doors propped open
2. Standard electrical wiring
3. Use of low-flame spread materials
4. Products-of-combustion detectors

4-31. Experience in fire fighting shows that the major factor in limiting fire damage is

1. prompt detection of fires
2. experienced fire fighters
3. multiple fire extinguishers
4. quick response time to alarms

4-32. During the third stage of a fire, fire fighting becomes increasingly difficult and often people cannot remain at the fire site for which of the following reasons?

1. Toxic gases only
2. High temperatures only
3. Large volume of smoke only
4. Toxic gases, high temperatures, and large volume of smoke

4-33. Prompt fire detection is best accomplished through the use of which of the following detectors?

1. Gas
2. Heat
3. Smoke
4. Flame

4-34. When detectors are installed, which of the following factors need NOT be considered?

1. The location of equipment
2. The direction and velocity of air flow
3. The presence of areas with stagnant air
4. The location of fire extinguishers

4-35. In the design of the detection control panel, which of the following indications should be included?

1. The power supply status of each detector
2. Which detector has alarmed
3. The cause of the alarm
4. What type of detector has alarmed

4-36. To assure that someone will be alerted to a fire, which of the following alarm locations is recommended as the primary location?

1. Computer room
2. Personnel office
3. Commanding officer's office
4. Buildinq maintenance

4-37. Reducing the sensitivity of the smoke detectors to eliminate nuisance alarms may have which of the following results?

1. Save energy
2. Extend equipment life
3. Delay fire detection
4. Cause poor personnel performance

4-38. In an actual fire situation, the air handling equipment could be shut down automatically to avoid which of the following problems?

1. Straining the air handling equipment
2. Excessive energy consumption
3. Excessive filter wear
4. Spreading smoke and fanning the flames

4-39. When fire detection systems are interconnected with air handling equipment, a preferred technique is to cause the system to take which of the following measures?

1. Exhaust the smoke
2. Lower the thermostat
3. Recirculate the smoke
4. Use inside air for intake

4-40. What is the minimum temperature required to activate an automatic sprinkler system?

1. 115°F
2. 125°F
3. 135°F
4. 145°F

4-41. To ensure the effectiveness of portable extinguishers, which of the following measures should be observed?

1. Extinguishers should be marked for rapid identification
2. Extinguishers should have inspection tags
3. Extinguishers should be placed in corners
4. Extinguishers should be placed on the floor, not mounted

4-42. Military personnel who are knowledgeable and trained in fire safety are needed by which of the following types of commands?

1. Small commands only
2. Medium commands only
3. Large commands only
4. Every command

4-43. When using supporting utilities, AIS technical managers should consider the probability of occurrence and the effects of which of the following conditions?

1. Vandalism only
2. Sabotage only
3. Fire only
4. Vandalism, sabotage, and fire

4-44. Excessive fluctuation in the dc voltage applied to the hardware can be caused if the line voltage is 90 percent or less of nominal for more than what minimum number of milliseconds?

1. 7
2. 6
3. 5
4. 4

4-45. Power fluctuations in line voltage cause unpredictable results in which of the following components?

1. Logic only
2. Hardware only
3. Data transfer only
4. Logic, hardware, and data transfer

4-46. In an AIS facility, the effects of internal power fluctuations can be minimized in which of the following ways?

1. Grounding the CPU
2. Isolating the AIS hardware from other facility loads
3. Wiring all components in parallel
4. Wiring each component with a circuit breaker

4-47. The technique of connecting the AIS facility to more than one utility feeder has more protection value when the feeders are connected in what manner?

1. To the same junction box
2. From the same utility pole
3. To different power substations
4. To different utility meters

4-48. An uninterrupted power supply (UPS) consists of a solid-state rectifier that performs which of the following functions?

1. Drives a solid-state inverter only
2. Keeps batteries charged only
3. Drives a solid-state inverter and keeps batteries charged
4. Synthesizes alternating current

4-49. The UPS battery supply can support a facility load for a maximum of how many minutes?

1. 35
2. 40
3. 45
4. 50

4-50. The control circuitry for a static transfer switch performs which of the following functions?

1. Senses variations in frequency
2. Senses an overcurrent condition
3. Switches the load to the alternate power source
4. Stops the flow of power

4-51. Using multiple, independent UPS units can provide which of the following benefits?

1. Power consumption is lowered
2. Each unit can be switched offline if it fails
3. The metering of component power consumption is facilitated
4. All of the above

4-52. If the risk analysis shows a major loss from power outages lasting 30 to 45 minutes or longer, which of the following measures should be taken?

1. Installing an on-site generator
2. Cutting back on operations
3. Relocating the facility
4. Adding more multiple, independent UPS units

4-53. Which of the following components must be large enough to support air-conditioning or minimum lighting as well as the UPS load?

1. Generator
2. Alternator
3. Prime mover
4. Alternate mover

4-54. Providing physical protection for an AIS facility involves which of the following processes?

1. Denying access to unauthorized persons
2. Permitting access to authorized persons
3. Both 1 and 2 above
4. Minimizing the risks of a natural disaster

4-55. Wherever AIS equipment is used for processing classified information, which of the following instructions should be used for applying physical protection and security policy?

1. OPNAVINST 5230.12
2. OPNAVINST 5239.1
3. SECNAVINST 5211.5
4. SECNAVINST 5233.1

4-56. Which of the following contingency plans for dealing with classified material should NOT be considered in emergencies?

1. Destruction
2. Protection
3. Removal
4. Reproduction

4-57. In an emergency, the placement of a perimeter guard force around the affected area provides protection in which of the following ways?

1. Provides external contact when communications are lost
2. Prevents the removal of classified material
3. Reduces the risk of additional destruction
4. Provides AIS access control

4-58. Which of the following methods may be used to protect the property boundary of the AIS facility?

1. Roving patrol only
2. Fencing-only
3. Roving patrol and fencing
4. Security badges

4-59. Fences installed for boundary protection should be (a) what minimum height with (b) what minimum number of strands of barbed wire?

1. (a) 8 feet (b) 2
2. (a) 8 feet (b) 3
3. (a) 10 feet (b) 2
4. (a) 10 feet (b) 3

4-60. Penetration sensors mounted on fences and gates should provide which of the following alarms when tripped?

1. External only
2. Internal only
3. External and internal

4-61. Tests show that electromagnetic or acoustic emanations from AIS hardware. may be intercepted up to a maximum of how many yards away?

1. 150
2. 230
3. 325
4. 400

4-62. If the AIS technical manager plans to take measures to control compromising emanations, those measures are subject to approval under the provisions of which of the following DOD directives?

1. 5200.19
2. C5200.19
3. 5200.28
4. C5200.28

4-63. The application of the measures to control compromising emanations within the industrial AIS systems is at the direction of the contracting activity concerned under the provisions of which of the following DOD directives?

1. 5200.19
2. C5200.19
3. 5200.28
4. C5200.28

4-64. The use of an intrusion detection system (IDS) in a protective program is covered in which of the following instructions?

1. OPNAVINST 5239.1
2. OPNAVINST 5510.1
3. SECNAVINST 5211.5
4. SECNAVINST 5233.1

4-65. The physical security requirements for a remote terminal area are based upon which of the following classifications?

1. The classification of the central computer facility
2. The classification of the remote terminal area
3. The classification of the data that will be accessed through the terminal
4. The classification assigned by higher authority

4-66. When the AIS system contains classified information, what action, if any, must be taken for each remote terminal that is not controlled?

1. Disconnect
2. Place offline
3. Turn off
4. None

4-67. In the annual security survey of an AIS facility, what is the second step?

1. Define and tabulate areas within the facility for control purposes
2. Evaluate all potential threats to the AIS facility
3. Identify areas where remedial measures are needed
4. Recommend improvements to upper management

4-68. When the annual security survey is conducted, it should begin at which of the following areas?

1. Roof
2. Basement
3. Perimeter
4. Top floor

4-69. When surveying the perimeter of the facility, the AIS technical manager need NOT check which of the following accessways?

1. Fire escapes
2. Doors and windows
3. Other entrances, such as vents
4. Manned posts at the property line

4-70. When surveying the internal security of a facility, the AIS technical manager should follow which of the following guidelines?

1. Begin the survey on the roof
2. Determine where alarms annunciate
3. Finish the survey in the mailroom area
4. Note the volume of the alarms

IN ANSWERING QUESTION 4-71, REFER TO TABLE 4-6 IN THE TEXT.

4-71. Which of the following questions need NOT be included in the physical security survey?

1. Is the present equipment up-to-date?
2. Is the alarm system inspected and tested occasionally to ensure operation?
3. What kind of sound does the alarm make?
4. How many zones of protection are within the protected building?

4-72. Which of the following facts are used by the AIS technical manager to evaluate existing access controls and protection measures?

1. The schedule of alarm tests
2. The design of the alarm system
3. The number and location of manned posts
4. The distance between the manned posts and the building

4-73. Which of the following items are prepared and executed for the accomplishment of the command’s specific mission?

1. Operation plans only
2. Operation plans and-the command’s organizational manual
3. Emergency response plans only
4. Emergency response plans and the command’s organizational manual

4-74. A total of how many different types of contingency plans make up a COOP security plan?

1. One
2. Two
3. Three
4. Four

4-75. The risk analysis should be reviewed by which of the following people?

1. Production control clerk
2. Response team
3. Technical manager
4. Upper management

ASSIGNMENT 5

Textbook Assignment: "AIS Security (continued)," chapter 4, pages 4-26 through 4-40; "General Security," chapter 5, pages 5-1 through 5-13.

5-1. The AIS technical manager can develop measures to use in case of emergency by reviewing operations and records with which of the following personnel?

1. Production control clerk
2. Response team members
3. Shift leaders
4. Users

5-2. All personnel should be instructed to take which of the following security measures if an evacuation of work areas is ordered?

1. Secure classified material in desks or file cabinets
2. Turn equipment and room lights off
3. Close the doors as areas are evacuated but leave the doors unlocked
4. Power up the air-conditioning equipment

5-3. To ensure that all safety requirements of the AIS facility are satisfied, the AIS technical manager and the operations division officer should review the protective plans with what frequency?

1. Monthly
2. Quarterly
3. Semiannually
4. Annually

5-4. Backup operations may take place onsite under which of the following conditions?

1. A partial loss of capability
2. Major damage only
3. Major destruction only
4. Major damaqe and destruction

5-5. For the purpose of making backup resources available, which of the following tasks can be set aside?

1. Short-term planning
2. Program development
3. Weekly processing
4. Backup processing

5-6. When backup alternatives are considered, which of the following substitute procedures may be implemented during an emergency?

1. A hard disk input could be used for a failed telephone input
2. Online processing could be substituted for batch processing
3. Print tapes could be carried to a backup facility for offline printing
4. Both 2 and 3 above

5-7. To evaluate alternate backup modes and offsite facilities, you should consider all but which of the following factors?

1. AIS hardware usage
2. Maintenance personnel for your AIS building
3. Overtime cost factor for civil service personnel
4. Transportation of personnel with needed supplies and materials

5-8. When developing the optimum backup plan, it is wise to form several backup plans, one of which has which of the following charac-teristics?

1. Extends beyond the cause of delay
2. Includes each minor partial failure
3. Lasts at least half the time required to reconstruct the facility
4. Includes one or more operating periods between minimum duration and worst case

5-9. Each COOP backup plan should cover a total of how many basic areas?

1. Five
2. Six
3. Three
4. Four

A. Administrative information
B. Computer system specifications
C. Performance specifications
D. User instructions

Figure 5A

IN ANSWERING QUESTIONS 5-10 THROUGH 5-12, SELECT FROM FIGURE 5A THE AREA OF THE COOP BACKUP PLAN DESCRIBED.

5-10. The specific ways in which performance of each task departs from normal is stated.

1. A
2. B
3. C
4. D

5-11. Input in different forms may be required.

1. A
2. B
3. C
4. D

5-12. The location of the system is given.

1. A
2. B
3. C
4. D

5-13. The process of recovery will be carried out more effectively and economically if handled by which of the following personnel?

1. The users only
2. The AIS staff only
3. The users and AIS staff
4. Personnel other than the AIS staff

5-14. Before recovery from total destruction is achieved, all but which of the following tasks must be completed?

1. Locating floor space for the AIS facility without regard for live load capacity
2. Verifying all needed hardware, equipment, and materials
3. Performing facility modifications
4. Procuring hardware

5-15. For COOP testing, a team should be assembled to perform all except which of the following tasks?

1. Prepare a scenario for the test
2. Control and observe the test
3. Evaluate the test results
4. Provide training

5-16. Which of the following is a standard for an AIS facility inspection?

1. It should be dependent and subjective
2. It should examine the information system and its use
3. It should ignore adequacy controls
4. It should be the first element in a physical security program

5-17. The characteristic of an inspection being independent and objective implies that the inspection has which of the following relationships to management?

1. Replaces normal management inspections
2. Is a part of normal management visibility
3. Complements normal management inspections
4. Is a substitute for the management reporting, system

5-18. An inspection can be expected to accomplish which of the following tasks?

1. Evaluate security controls for the AIS facility
2. Provide users an opportunity to maintain the AIS security program
3. Provide the impetus to keep workers and management complacent
4. Uncover adequate operational areas

5-19. In determining the frequency of internal inspections, the AIS technical manager should consider which of the followinq factors?

1. Operation workload
2. The rate of change of the AIS
3. The SOPS of the AIS staff
4. The results of the last inspection only

5-20. What is the role of the inspection team?

1. To develop security controls
2. To evaluate established controls
3. To enforce control procedures
4. To develop security procedures

5-21. Which of the following characteristics of the inspection board members will NOT affect the success of the inspection?

1. Ability
2. Objectivity
3. Probing nature
4. Punctuality

5-22. Which of the following is NOT an important characteristic for the inspection board members?

1. Ability to enforce controls
2. Attention to detail
3. Inquisitiveness
4. Probing nature

5-23. Which of the following types of expertise is helpful for a member of the inspection team?

1. Operations experience only
2. Security experience only
3. Security experience and programming knowledge
4. Operations experience and programming knowledge

5-24. The group of people who have the most to gain from an effective inspection are the

1. members of the inspection team
2. members of the security force
3. programmers in the facility
4. users of the facility

5-25. Which of the following is a characteristic of a comprehensive inspection plan?

1. It is action-oriented
2. It lists actions to be bypassed
3. It is tailored for universal installation
4. It allows freedom in the report design

5-26. In developing a comprehensive inspection plan, what is the third step?

1. Review the risk analysis plan
2. Examine the security policy and extract pertinent objectives
3. Examine the AIS facility organization chart and job descriptions
4. Review documents to determine the specified security operating procedures

5-27. When formulating the inspection program, which of the following areas is the most important to consider?

1. The most recent security breach without regard for security priorities
2. The activities that produce minimum results with the most effort
3. The critical issues with regard to security
4. The measures that are tested most frequently in day-to-day operations

5-28. It is considered advantageous to test fire detection sensors under surprise conditions for which of the following reasons?

1. To test the response to alarms
2. To test the reaction of the fire party
3. To test the effectiveness of evacuation plans
4. Each of the above

5-29. Why should the review of previous inspection reports be part of the process of developing an inspection plan?

1. To show trends
2. To identify weaknesses that should have been corrected
3. To identify strengths that were identified
4. To identify previous team members

5-30. With what frequency should a scheduled inspection take place?

1. Monthly
2. Quarterly
3. Semiannually
4. Annually

5-31. A surprise inspection should be approved by which of the following personnel?

1. The facility security officer
2. The AIS technical manager
3. The commanding officer of the command in charge of the AIS facility
4. The commanding officer of the user command

5-32. In conducting a scheduled inspection, which of the following is normally the first step?

1. Interviewing the AIS personnel
2. Scrutinizing the AIS facility records
3. Inventorying the AIS hardware capabilities of the facility
4. Testing the AIS facility access control procedures

5-33. Most security inspections include testing which of the following activities at AIS facilities?

1. Fire-fighting procedures
2. Facility evacuation
3. System backup
4. Personnel placement procedures

5-34. What is the preferred frequency at which the inspection team should convene to review progress and compare notes?

1. At the end of each day’s activity
2. At the end of each week’s activities
3. Every 2 weeks
4. Every 3 weeks

5-35. After the completion of the inspection, when should the written report be prepared?

1. When requested by the supervisor of the AIS facility being inspected
2. When requested by the commanding officer of the AIS facility being inspected
3. Immediately after the inspection, while the impressions are still fresh
4. After an extended period of time to allow the inspection team members to reflect on the inspection process

5-36. Who is responsible for implementing the recommendations received from the inspection?

1. The AIS technical manager
2. The security officer
3. The commanding officer
4. The TYCOM

5-37. The best approach in assigning responsibilities for corrective action is to summarize each major deficiency on a control sheet outlining which of the following areas?

1. An executive summary
2. The action taken or required
3. The date the deficiency was discovered
4. The reporting official

5-38. For any control item that is still open, it is recommended that reports be turned in to upper management with what frequency?

1. Weekly
2. Monthly
3. Quarterly
4. Semiannually

5-39. Which of the following instructions provides guidelines for implementing security safeguards required to implement the Privacy Act of 1974?

1. SECNAVINST 5211.5
2. SECNAVINST 5239.2
3. OPNAVINST 5510.1
4. OPNAVINST 5239.1

5-40. Which of the following subsections of the Privacy Act (title 5, section 552a) requires the use of safeguards to ensure the confidentiality and security of records?

1. Subsection (b)
2. Subsection (c)
3. Subsection (e) (5)
4. Subsection (e) (10)

5-41. A personal data security risk assessment benefits a command in all but which of the following ways?

1. It saves money that might have been wasted on safeguards that do not significantly lower the overall data risks
2. It ensures that additional security safeguards help to counter all the serious personal data security risks
3. It provides a basis for deciding whether additional security safeguards are needed for personal data
4. It considers only the risks to personal data

5-42 . Which of the following participants should NOT be included on the risk assessment team?

1. A representative of the operating facility
2. An individual responsible for security
3. A system programmer
4. A systems analyst

5-43. Data may be misrouted, mis-labeled, or it may contain unexpected personal information as a result of which of the following data security risks?

1. Input errors
2. Program errors
3. Improper data dissemination
4. Mistaken processing of data

5-44. When security measures to adequately control system access to personal data are developed, they should include protection from all except which of the following risks?

1. Dial-in access
2. Open system access
3. Physical destruction of the AIS
4. Unprotected files and theft of data

5-45. Commands designing large computer networks should consider which of the following risks early in the planning stages?

1. Eavesdropping only
2. Misidentified access and eavesdropping only
3. Operating system flaws and subverting programs only
4. Misidentified access, eavesdropping, operating systems flaws, subverting programs, and spoofing

5-46. Information management practices include all but which of the following activities?

1. Data collection, validation, and transformation
2. Information processing or handling
3. Information control, display, and presentation
4. Managerial determination of the need and use of the information

5-47. Which of the following practices is/are suggested for the handling of personal data?

1. Label recording media that contain data of local personnel only
2. Carefully control products of intermediate processing steps
3. Maintain an online, up-to-date hardcopy authorization list of all individuals who have access to any data
4. Both 2 and 3 above

5-48. Which of the following practices is/are suggested for the maintenance of personal records?

1. Establish procedures for maintaining correct, current accounting of all new personal data brought into the computer facility
2. Maintain logbooks for terminals that are used to access any data by system users
3. Both 1 and 2 above
4. Log each transfer of storage media containing data to the computer facility

5-49. For a broader knowledge of personal identification and identification techniques, you should refer to which of the FIPS publications?

1. FIPS PUB 31
2. FIPS PUB 48
3. FIPS PUB 79
4. FIPS PUB 114

5-50. Which of the following pieces of equipment might be considered a TEMPEST hazard?

1. Personal computer
2. Electric typewriter
3. Both 1 and 2 above
4. A copying machine

5-51. The vulnerability of a ship or aircraft can be determined by which of the following means?

1. A TEMPEST survey
2. A TEMPEST vulnerability assessment
3. A TEMPEST investigation
4. An emission control test

5-52. What is the purpose of EMCON?

1. To intercept and rebroadcast signals to confuse hostile forces
2. To prevent hostile forces from detecting, identifying, and locating friendly forces
3. To minimize the amount of transmission time on live circuits
4. Both 2 and 3 above

4-53. What is the designation of security spaces requiring access control?

1. Controlled area
2. Exclusion area
3. Restricted area
4. Limited area

4-54. Which of the following information should appear in a visitors log for a communications center?

1. Visitor’s printed name and signature
2. Purpose of visit and the escort’s name
3. Date and time of visit
4. Each of the above

5-55. The combination to a classified material container must be changed at what maximum interval?

1. Monthly
2. Every 6 months
3. Every 12 months
4. Every 24 months

5-56. Which of the following statements concerning the security classification of a safe combination is correct?

1. All combinations are classified Secret regardless of the classification of contents stored within
2. All combinations are classified Confidential regardless of the classification of contents stored within
3. All combinations are handled as official information
4. Combinations are assigned a security classification equal to the highest category of classified material stored

5-57. An individual who is responsible for safeguarding and accounting for classified material is known by what term?

1. Custodian
2. User
3. Keeper
4. Guardian

5-58. Which of the following conditions for protecting classified material after workinq hours is NOT in accordance with security instructions?

1. Classified documents are in locked authorized containers
2. Classified notes, carbon paper, typewriter ribbons, and rough drafts have been destroyed or are in locked authorized containers
3. The contents of wastebaskets containing classified material were not burned, but are in locked authorized containers
4. Burn bags, ready for burning the next day, are securely stapled, numbered, and neatly lined up along the bulkhead

5-59. What is the minimum number of times the dial of a security container must be rotated in the same direction to ensure it is locked?

1. Five
2. Two
3. Three
4. Four

5-60. During routine destruction of classified material, what is the ultimate goal of the destruction?

1. To clear files of old material so there is more room for new material
2. To make reconstruction of the material impossible
3. To prevent unauthorized reproduction
4. To destroy the material as quickly as possible

5-61. What is the most efficient means of destroying classified material?

1. Burning
2. Shredding
3. Jettisoning
4. Pulping

5-62. Persons witnessing destruction of classified material must have a security clearance of at least what level?

1. Confidential
2. Secret
3. Top Secret
4. The level of the material being destroyed

5-63. When is a record of destruction required for Secret messages?

1. If only one person performs destruction
2. If the messages have special markings
3. If the messages have to be jettisoned
4. During routine destruction

5-64. Records of destruction of classified material must be maintained for what minimum length of time?

1. 1 yr
2. 2 yr
3. 6 mo
4. 18 mo

5-65. How are burn bags accounted for prior to burning?

1. Bags are placed in a secure place and inventoried daily
2. Each bag must be serially numbered and a record kept of all subsequent handling until destroyed
3. Each office is responsible for its burn bag until the day of destruction
4. On the day of destruction, each bag is serially numbered

5-66. What is the maximum allowable size of material shredded by a crosscut shredding machine?

1. 1/32 inch wide by 1 inch long
2. 1/32 inch wide by 1/2 inch long
3. 3/64 inch wide by 1/2 inch long
4. 3/64 inch wide by 1 inch long

5-67. If classified material must be jettisoned during emergency destruction, what should be the minimum depth of the water?

1. 500 fathoms
2. 700 fathoms
3. 1,000 fathoms
4. 5,000 fathoms

5-68. Which of the following areas must be covered in a command's emergency action plan?

1. Enemy actions
2. Civil disturbances
3. Natural disasters
4. Each of the above

5-69. When a command implements its emergency plan, the priority of destruction should be based on what factor?

1. The speed at which the material can be destroyed
2. The amount of material that can be destroyed in the least amount of time
3. The potential effect on national security should the material fall into hostile hands
4. The number of personnel required for destruction

5-70. When an emergency plan is implemented, which of the following material should be destroyed first?

1. SPECAT material
2. Special access material
3. COMSEC material
4. PERSONAL FOR material

5-71. In addition to having an emergency destruction plan, all commands are required to have what other type of emergency plan?

1. Fire
2. Evacuation
3. Security force
4. Watch security

5-72. Which of the following material should NOT be destroyed during a precautionary destruction?

1. Material of a historical nature
2. Material that has been superseded
3. Material essential to communications
4. Material that is unneeded

5-73. What should be done with superseded classified material?

1. Retain indefinitely
2. Retain for two years, then destroy
3. Retain for one month, then destroy
4. Destroy in accordance with its prescribed time frame

STUDENT COMMENT SHEET

THIS FORM MAY BE USED TO SUGGEST IMPROVEMENTS, REPORT COURSE ERRORS, OR TO REQUEST HELP IF YOU HAVE DIFFICULTY COMPLETING THE COURSE.

NOTE: IF YOU HAVE NO COMMENTS, YOU DO NOT HAVE TO SUBMIT THIS FORM.

Date_____

FROM:

_____
RATE/RANK/GRADE, NAME (FIRST, M.I., LAST)

DSN:_____
_____ Commercial:_____
STREET ADDRESS, APT # FAX:_____
INTERNET:_____

_____
CITY, STATE, ZIP CODE

To. COMMANDING OFFICER
NETPDTC CODE N311
6490 SAUFLEY FIELD RD
PENSACOLA FL 32509-5237

Subj: RADIOMAN TRAINING SERIES, MODULE 1- ADMINISTRATION AND SECURITY, NAVEDTRA 12845

1. The following comments are hereby submitted:

PRIVACY ACT STATEMENT

UNDER AUTHORITY OF TITLE 5, USC 301, INFORMATION REGARDING YOUR MILITARY STATUS IS REQUESTED TO ASSIST IN PROCESSING YOUR COMMENTS AND IN PREPARING A REPLY. THIS INFORMATION WILL NOT BE DIVULGED WITHOUT WRITTEN AUTHORIZATION TO ANYONE OTHER THAN THOSE WITHIN DOD FOR OFFICIAL USE IN DETERMINING PERFORMANCE.

. . . . . (Fold along dotted line . . . . . .

. . . . . (Fold along dotted fine) . . . . . .

DEPARTMENT OF THE NAVY

COMMANDING OFFICER
NETPDTC CODE N311
6490 SAUFLEY FIELD RD
PENSACOLA FL 32509-5237

OFFICIAL BUSINESS

COMMANDING OFFICER
NETPDTC CODE N311
6490 SAUFLEY FIELD RD
PENSACOLA FL 32509-5237

NAVEDTRA 1430/5
Stock Ordering No. 0502-LP-216-0100

PRINT OR TYPE

TITLE_____ NAVEDTRA_____

NAME_____ ADDRESS_____
Last First Middle Street/Ship/Unit/Division, etc.

_____
City or FPO State Zip

RANK/RATE_____ SSN_____ DESIGNATOR_____ ASSIGNMENT NO._____ DATE SUBMITTED _____

☐ USN ☐ USNR ☐ ACTIVE ☐ INACTIVE OTHER (Specify)_____

SCORE

	1 T	2 F	3	4			1 T	2 F	3	4			1 T	2 F	3	4	
1	☐	☐	☐	☐	_____	26	☐	☐	☐	☐	_____	51	☐	☐	☐	☐	_____
2	☐	☐	☐	☐	_____	27	☐	☐	☐	☐	_____	52	☐	☐	☐	☐	_____
3	☐	☐	☐	☐	_____	28	☐	☐	☐	☐	_____	53	☐	☐	☐	☐	_____
4	☐	☐	☐	☐	_____	29	☐	☐	☐	☐	_____	54	☐	☐	☐	☐	_____
5	☐	☐	☐	☐	_____	30	☐	☐	☐	☐	_____	55	☐	☐	☐	☐	_____
6	☐	☐	☐	☐	_____	31	☐	☐	☐	☐	_____	56	☐	☐	☐	☐	_____
7	☐	☐	☐	☐	_____	32	☐	☐	☐	☐	_____	57	☐	☐	☐	☐	_____
8	☐	☐	☐	☐	_____	33	☐	☐	☐	☐	_____	58	☐	☐	☐	☐	_____
9	☐	☐	☐	☐	_____	34	☐	☐	☐	☐	_____	59	☐	☐	☐	☐	_____
10	☐	☐	☐	☐	_____	35	☐	☐	☐	☐	_____	60	☐	☐	☐	☐	_____
11	☐	☐	☐	☐	_____	36	☐	☐	☐	☐	_____	61	☐	☐	☐	☐	_____
12	☐	☐	☐	☐	_____	37	☐	☐	☐	☐	_____	62	☐	☐	☐	☐	_____
13	☐	☐	☐	☐	_____	38	☐	☐	☐	☐	_____	63	☐	☐	☐	☐	_____
14	☐	☐	☐	☐	_____	39	☐	☐	☐	☐	_____	64	☐	☐	☐	☐	_____
15	☐	☐	☐	☐	_____	40	☐	☐	☐	☐	_____	65	☐	☐	☐	☐	_____
16	☐	☐	☐	☐	_____	41	☐	☐	☐	☐	_____	66	☐	☐	☐	☐	_____
17	☐	☐	☐	☐	_____	42	☐	☐	☐	☐	_____	67	☐	☐	☐	☐	_____
18	☐	☐	☐	☐	_____	43	☐	☐	☐	☐	_____	68	☐	☐	☐	☐	_____
19	☐	☐	☐	☐	_____	44	☐	☐	☐	☐	_____	69	☐	☐	☐	☐	_____
20	☐	☐	☐	☐	_____	45	☐	☐	☐	☐	_____	70	☐	☐	☐	☐	_____
21	☐	☐	☐	☐	_____	46	☐	☐	☐	☐	_____	71	☐	☐	☐	☐	_____
22	☐	☐	☐	☐	_____	47	☐	☐	☐	☐	_____	72	☐	☐	☐	☐	_____
23	☐	☐	☐	☐	_____	48	☐	☐	☐	☐	_____	73	☐	☐	☐	☐	_____
24	☐	☐	☐	☐	_____	49	☐	☐	☐	☐	_____	74	☐	☐	☐	☐	_____
25	☐	☐	☐	☐	_____	50	☐	☐	☐	☐	_____	75	☐	☐	☐	☐	_____

THIS FORM MAY BE LOCALLY REPRODUCED